KASPERSKY LAB

Kaspersky® Anti-Virus 6.0 para Windows Servers

MANUAL DE UTILIZADOR

KASPERSKY ANTI-VIRUS PARA WINDOWS SERVERS 6.0

Manual de utilizador

© Kaspersky Lab
http://www.kaspersky.com

Data de Revisão: Julho, 2007

Índice

CAPÍTULO 1. AMEAÇAS À SEGURANÇA DO COMPUTADOR 9
1.1. Fontes de ameaças 9
1.2. Como se espalham as ameaças 10
1.3. Tipos de ameaças 12

CAPÍTULO 2. KASPERSKY ANTI-VIRUS PARA WINDOWS SERVERS 6.0 15
2.1. O que há de novo no Kaspersky Anti-Virus para Windows Servers 6.0 15
2.2. Como é constituída a Protecção do Kaspersky Anti-Virus para Windows Servers 17
2.2.1. Anti-Vírus de Ficheiros 17
2.2.2. Tarefas de verificação de vírus 17
2.2.3. Ferramentas do programa 18
2.3. Requisitos de hardware e software de sistema 20
2.4. Pacotes de software 20
2.5. Suporte para utilizadores registados 21

CAPÍTULO 3. INSTALAÇÃO DO KASPERSKY ANTI-VIRUS PARA WINDOWS SERVERS 6.0 23
3.1. Procedimento de instalação usando o Assistente de Instalação 24
3.2. Assistente de Configuração 28
3.2.1. Utilizar ficheiros guardados da Versão 5.0 28
3.2.2. Activar o programa 29
3.2.2.1. Seleccionar o método de activação do programa 29
3.2.2.2. Inserir o código de activação 30
3.2.2.3. Obter um Ficheiro da Chave 30
3.2.2.4. Seleccionar o ficheiro da chave de licença 31
3.2.2.5. Concluir a activação do programa 31
3.2.3. Configurar as definições de actualização 31
3.2.4. Configurar verificações de vírus agendadas 32
3.2.5. Restringir o acesso ao programa 33
3.2.6. Finalizar o Assistente de Configuração 33
3.3. Instalar o programa a partir da linha de comandos 34

3.4. Procedimento para instalar o Objecto de Política de Grupo 35
3.4.1. Instalar o programa 35
3.4.2. Actualizar o programa 36
3.4.3. Desinstalar o programa 36
3.5. Actualizar da versão 5.0 para a versão 6.0 37

CAPÍTULO 4. INTERFACE DO PROGRAMA 38
4.1. Ícone de bandeja do sistema 38
4.2. O menu de contexto 39
4.3. Janela principal do programa 40
4.4. Janela de definições do programa 42

CAPÍTULO 5. COMO COMEÇAR 44
5.1. Qual o estado da protecção que o meu computador tem? 44
5.1.1. Indicadores de protecção 45
5.1.2. Estado da componente Kaspersky Anti-Virus para Windows Servers 48
5.1.3. Estatísticas de funcionamento do programa 49
5.2. Como verificar a existência de vírus no seu servidor 50
5.3. Como verificar as áreas críticas do computador 51
5.4. Como verificar a existência de vírus num ficheiro, pasta ou disco 51
5.5. Como actualizar o Programa 52
5.6. O que fazer se a protecção não estiver a funcionar 53

CAPÍTULO 6. SISTEMA DE GESTÃO DA PROTECÇÃO 55
6.1. Parar e Retomar a protecção no seu computador 55
6.1.1. Pausar a protecção 56
6.1.2. Desactivar a protecção do servidor 57
6.1.3. Pausar / parar a protecção 58
6.1.4. Restaurar a protecção no seu computador 58
6.1.5. Encerrar o programa 59
6.2. Tipos de programas maliciosos a monitorizar 59
6.3. Criar uma zona confiável 60
6.3.1. Regras de exclusão 61
6.3.2. Aplicações confiáveis 65
6.4. Iniciar tarefas com outro perfil 67
6.5. Configurar Tarefas e Notificações Agendadas 68
6.6. Opções de energia 70

6.7. Configuração de servidor multi-processador 71

CAPÍTULO 7. PROTECÇÃO ANTI-VÍRUS DO SISTEMA DE FICHEIROS DO SERVIDOR 73
7.1. Seleccionar um nível de segurança dos ficheiros 74
7.2. Configurar o Anti-Vírus de Ficheiros 76
7.2.1. Definir os tipos de ficheiros a serem verificados 76
7.2.2. Definir o âmbito de protecção 79
7.2.3. Configurar definições avançadas 80
7.2.4. Restaurar as predefinições do Anti-Vírus de Ficheiros 83
7.2.5. Seleccionar acções para objectos 83
7.2.6. Criar um modelo de notificação 85
7.3. Desinfecção adiada 86

CAPÍTULO 8. VERIFICAÇÃO DE VÍRUS NO SEU COMPUTADOR 87
8.1. Gerir tarefas de verificação de vírus 88
8.2. Criar uma lista de objectos a verificar 88
8.3. Criar tarefas de verificação de vírus 90
8.4. Configurar tarefas de verificação de vírus 91
8.4.1. Seleccionar um nível de segurança 92
8.4.2. Definir os tipos de ficheiros a verificar 93
8.4.3. Restaurar as definições de verificação predefinidas 96
8.4.4. Seleccionar acções para objectos 97
8.4.5. Definições avançadas de verificação de vírus 99
8.4.6. Estabelecer definições globais para todas as tarefas de verificação 101

CAPÍTULO 9. TESTAR O KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS SERVERS 102
9.1. O vírus de teste EICAR e as suas variantes 102
9.2. Testar o Anti-Vírus de Ficheiros 104
9.3. Testar as tarefas de verificação de vírus 105

CAPÍTULO 10. ACTUALIZAÇÕES DO PROGRAMA 107
10.1. Iniciar o Actualizador 108
10.2. Reverter para a actualização anterior 109
10.3. Criar tarefas de actualização 109
10.4. Configurar as definições de actualização 111
10.4.1. Seleccionar uma origem de actualização 111

10.4.2. Seleccionar o método de actualização e o que actualizar ... 114
10.4.3. Configurar as definições de ligação de rede ... 116
10.4.4. Distribuição de actualizações ... 118
10.4.5. Acções depois de actualizar o programa ... 119

CAPÍTULO 11. OPÇÕES AVANÇADAS ... 121
11.1. Quarentena para objectos potencialmente infectados ... 122
11.1.1. Acções com objectos em quarentena ... 123
11.1.2. Configurar a Quarentena ... 125
11.2. Cópias de segurança de objectos perigosos ... 125
11.2.1. Acções com cópias de segurança ... 126
11.2.2. Configurar as definições de Cópia de Segurança ... 128
11.3. Relatórios ... 128
11.3.1. Configurar as definições dos relatórios ... 131
11.3.2. Separador *Detectadas* ... 132
11.3.3. Separador *Eventos* ... 133
11.3.4. Separador *Estatísticas* ... 134
11.3.5. Separador *Definições* ... 135
11.3.6. Separador *Utilizadores banidos* ... 136
11.4. Informação geral sobre o programa ... 136
11.5. Gerir licenças ... 137
11.6. Suporte Técnico ... 139
11.7. Configurar a Interface do Kaspersky Anti-Virus para Windows Servers ... 141
11.8. Utilizar as opções avançadas ... 143
11.8.1. Notificações de eventos do Kaspersky Anti-Virus para Windows Servers ... 144
11.8.1.1. Tipos de eventos e métodos de entrega das notificações ... 145
11.8.1.2. Configurar notificações por e-mail ... 146
11.8.1.3. Configurar definições de registo de eventos ... 147
11.8.2. Autodefesa e restrição de acesso ... 148
11.8.3. Resolver conflitos com outras aplicações ... 150
11.9. Importar e exportar as definições do Kaspersky Anti-Virus para Windows Servers ... 150
11.10. Repor as predefinições ... 151

CAPÍTULO 12. ADMINISTRAR O PROGRAMA COM O KASPERSKY ADMINISTRATION KIT ... 152
12.1. Administrar a aplicação ... 154

12.1.1. Iniciar/parar a aplicação 155
12.1.2. Configurar as definições da aplicação 156
12.1.3. Configurar definições específicas 158
12.2. Gerir tarefas 159
12.2.1. Iniciar e parar tarefas 160
12.2.2. Criar tarefas 161
12.2.2.1. Criar tarefas locais 161
12.2.2.2. Criar tarefas de grupo 163
12.2.2.3. Criar tarefas globais 164
12.2.3. Configurar definições de tarefas 164
12.3. Gerir políticas 166
12.3.1. Criar políticas 166
12.3.2. Ver e editar definições da política 168

CAPÍTULO 13. TRABALHAR COM O PROGRAMA A PARTIR DA LINHA DE COMANDOS 170
13.1. Activar a aplicação 171
13.2. Gerir o Anti-Vírus de Ficheiros e tarefas 172
13.3. Verificação Anti-Virus 175
13.4. Actualizações do programa 179
13.5. Definições de reversão 180
13.6. Exportar definições 181
13.7. Importar definições 182
13.8. Iniciar o programa 183
13.9. Parar o programa 183
13.10. Obter um Ficheiro de Rastreio 183
13.11. Visualizar o Menu Ajuda 184
13.12. Códigos de retorno da interface da linha de comandos 184

CAPÍTULO 14. MODIFICAR, REPARAR E REMOVER O PROGRAMA 186
14.1. Modificar, reparar e remover o programa com o Assistente de Instalação 186
14.2. Desinstalar o programa a partir da linha de comandos 189

APÊNDICE A. INFORMAÇÃO DE REFERÊNCIA 190
A.1. Lista de ficheiros verificados por extensão 190
A.2. Máscaras de exclusão de ficheiros possíveis 192
A.3. Possíveis máscaras de exclusão de ameaças 194
A.4. Resumo das definições no ficheiro *setup.ini* 194

APÊNDICE B. KASPERSKY LAB 196
B.1. Outros produtos da Kaspersky Lab 197
B.2. Contacte-nos 209

APÊNDICE C. CONTRATO DE LICENÇA 210

CAPÍTULO 1. AMEAÇAS À SEGURANÇA DO COMPUTADOR

O número de crimes destinados a quebrar a segurança da informação cresceu, dado que as tecnologias de informação desenvolveram-se rapidamente e penetraram em todos os aspectos da existência humana.

Os criminosos do ciberespaço demonstraram grande interesse na actividade das estruturas estatais e dos empreendimentos comerciais. Fazem tentativas de roubo e divulgação de informação confidencial, destruindo reputações de empresas, quebrando a continuidade de negócios e danificando, por consequência, os recursos informativos de uma organização. Estes actos podem causar danos extensivos a bens, tanto tangíveis, como intangíveis.

Não são apenas as grandes companhias que correm riscos. Os utilizadores individuais também podem ser atacados. Usando várias ferramentas, os criminosos ganham acesso a dados pessoais (contas bancárias, números de cartões de crédito e passwords), provocam avarias no seu sistema ou obtêm acesso completo ao seu computador. Esse computador pode depois ser usado como parte de uma rede zombie, uma rede de computadores infectados usados pelos hackers para atacar servidores, enviar spam, colher informação confidencial e espalhar novos vírus e cavalos de tróia (Trojans).

No mundo de hoje, todos reconhecem que a informação é um bem valioso que deverá ser protegido. Ao mesmo tempo, a informação deve estar acessível a um determinado grupo de utilizadores (por exemplo, empregados, clientes e parceiros de um negócio). Esta é a razão porque há uma necessidade de criar um sistema de segurança de informação global. Este sistema deverá tomar em conta todas as possíveis fontes de ameaças, quer sejam humanas, feitas pelo Homem, ou acidente naturais, e usar uma série completa de medidas defensivas, a nível físico, administrativo e de software.

1.1. Fontes de ameaças

Uma pessoa, um grupo de pessoas, ou mesmo alguns fenómenos não relacionados com a actividade humana, poderão servir como uma ameaça à segurança de informação. Deste modo, todas as fontes de ameaças dividem-se em três grupos:

- **O factor humano**. Este grupo de ameaças diz respeito às acções de pessoas com acesso autorizado ou não-autorizado à informação. As ameaças neste grupo podem ser divididas em:
    - *Externas*, incluindo criminosos do ciberespaço, hackers, fraudes na Internet, sócios pouco escrupulosos e estruturas criminais.
    - *Internas*, incluindo acções de empregados da empresa. As acções tomadas por este grupo podem ser deliberadas ou acidentais.
- **O factor tecnológico**. Este grupo de ameaças está ligado a problemas técnicos – equipamento usado que se tornou obsoleto e a má qualidade de software e hardware de processamento de informação. Tudo isto leva a avarias de equipamento e a perdas frequentes de dados.
- **O factor do desastre natural**. Este grupo de ameaça inclui qualquer número de ocorrências levadas a cabo pela Natureza e outras ocorrências independentes da actividade humana.

Todas as três fontes de ameaças devem ser tomadas em conta quando se desenvolver um sistema de segurança de protecção de dados. Este manual de utilizador apenas cobre o que está directamente ligado à experiência da Kaspersky Lab – ameaças externas envolvendo actividade humana.

1.2. Como se espalham as ameaças

À medida que a moderna tecnologia de computadores e ferramentas de comunicação se desenvolvem, os hackers têm mais oportunidades para espalhar ameaças. Vejamo-las mais de perto:

A Internet

A Internet é única, dado que não é propriedade de ninguém e não tem limites geográficos. Promoveu de vários modos o desenvolvimento de inúmeros recursos da Internet e a troca de informação. Hoje, qualquer um pode aceder a dados na Internet ou criar a sua própria página Web.

Contudo, estas mesmas funções da Web mundial dão aos hackers a capacidade para cometer crimes na Internet, tornando-os difíceis de detectar e punir enquanto são efectuados.

Os hackers colocam vírus e outros programas maliciosos em páginas de Internet e disfarçam-nas como utilitários úteis gratuitos. Adicionalmente, scripts que sejam automaticamente executados quando abre determinadas páginas de Internet podem agir perigosamente no seu

computador, incluindo a modificação do registo do sistema, o roubo de dados pessoais e instalação de software malicioso.

Ao utilizar tecnologias de rede, os hackers podem atacar servidores de empresas. Estes ataques podem levar a que partes do seu sistema funcionem mal ou podem dar aos hackers um acesso completo ao seu sistema e à informação guardada nele. Também podem usá-lo como parte de uma rede zombie.

Intranet

A intranet é a rede interna, concebida especificamente para tratar de informação no seio da empresa ou numa rede doméstica. Uma intranet é um espaço unificado para guardar, trocar e aceder à informação em todos os computadores da rede. Isto significa que, se um dos computadores da rede estiver infectado, os outros correm um grande risco de infecção. Para evitar essas situações, quer o perímetro da rede, quer cada computador individual devem estar protegidos.

E-mail

Dado que, praticamente, todos os computadores têm clientes de e-mail instalados e visto que programas maliciosos exploram o conteúdo das agendas electrónicas, existem condições apropriadas para espalhar programas maliciosos. O utilizador de um computador infectado, estando alheado do facto, pode enviar e-mails infectados a amigos ou colegas, que por sua vez enviam mais e-mails infectados. É habitual que documentos infectados fiquem indetectados e sejam enviados com informação de negócios de uma grande empresa. Quando isto acontece, mais do que um punhado de pessoas são infectadas. Podem ser centenas ou milhares, todas a enviar ficheiros infectados a dezenas de milhares de assinantes.

Meios amovíveis de armazenamento

Meios amovíveis (disquetes, CD/DVD-ROMs e unidades de armazenamento USB) são amplamente usadas para guardar e transmitir informação.

Ao abrir um ficheiro com código malicioso, a partir de um meio amovível de armazenamento, poderá danificar dados guardados no computador e espalhar vírus pelas outras unidades do computador ou outros computadores da rede.

1.3. Tipos de ameaças

Existe um grande número de ameaças que podem afectar hoje o computador. Esta secção abordará as ameaças que o Kaspersky Anti-Virus para Windows Servers bloqueia.

Vermes (Worms)

Esta categoria de programa malicioso explora, amplamente, as vulnerabilidades do sistema operativo para se espalhar. A classe foi designada devido ao modo como os worms (vermes) passam de computador para computador, usando redes e e-mails. Esta capacidade dá aos worms uma maior velocidade para se espalharem.

Os worms penetram num computador, procuram os endereços de rede de outros computadores e enviam uma quantidade de cópias por si executadas para esses endereços. Para além disso, os worms utilizam com frequência dados de agendas de endereços de clientes de e-mail. Alguns destes programas maliciosos criam por vezes ficheiros de trabalho em discos de sistema, mas podem ser executados sem quaisquer recursos de sistema (com excepção da memória RAM).

Vírus

Programas que infectaram outros programas, juntando-lhes o seu próprio código para ganhar controlo de ficheiros infectados quando estes são abertos. Esta definição simples explica a acção fundamental executada por um vírus – *infecção*.

Cavalos de Tróia (Trojans)

Programas que executam acções não autorizadas em computadores, como, por exemplo, apagar informação em unidades, provocando o bloqueio do sistema, roubar informação confidencial, etc. Esta classe de programas maliciosos não é um vírus no sentido tradicional do termo (significando que não infecta outros computadores ou dados). Os cavalos de Tróia (Trojans) não podem entrar em computadores por si só e são espalhados por hackers, que os disfarçam de software comum. Os danos que podem trazer podem exceder várias vezes os ataques de vírus tradicionais.

Recentemente, os worms têm sido o tipo de programa malicioso mais espalhado para danificar dados de computadores. Depois seguem-se os vírus e cavalos de Tróia. Alguns programas maliciosos combinam funções de dois ou mesmo três destas classes.

Software com publicidade (Adware)

Código de programa incluído no software, desconhecido para o utilizador, concebido para mostrar anúncios. O adware está habitualmente incorporado no software de livre distribuição. A publicidade está situada na interface do programa. Estes programas reúnem com frequência dados pessoais do utilizador e enviam-nos para o programador, alteram as definições do navegador (páginas de abertura e de pesquisa, níveis de segurança, etc.) e criam tráfego que o utilizador não pode controlar. Tudo isto pode levar à quebra da política de segurança e a perdas financeiras directas.

Software espião (Spyware)

Software que recolhe informação sobre um utilizador em particular ou organização sem o seu conhecimento. Poderá nunca saber que tem spyware instalado no seu computador. Em geral, o objectivo do spyware é:

- registar as acções do utilizador num computador
- reunir informação sobre o conteúdo do seu disco rígido; nestes casos, envolve a busca de alguns directórios e o registo do sistema para compilar uma lista do software instalado no computador
- reunir informação sobre a qualidade da ligação de rede, a largura de banda, a velocidade do modem, etc.

Software potencialmente perigoso (Riskware)

O riskware é software, potencialmente, perigoso que não tem uma função maliciosa, mas que pode ser usado por hackers como componente auxiliar para um programa malicioso, dado que contém falhas e erros. Sobre certas condições, ter estes programas no computador poderá pôr os seus dados em risco. Estes programas incluem, por exemplo, algumas utilidades para administração remota, programas de alternância automática da disposição do teclado, clientes de IRC, servidores FTP e utilitários gerais para parar processos ou esconder o seu funcionamento.

Outro tipo de programa malicioso, que acompanha programas como adware, spyware e riskware, são os programas que se instalam no navegador da Web e redireccionam o tráfego.

Programas de brincadeiras (Jokes)

Software que não tenta fazer qualquer dano directo, mas exibe mensagens que afirmam já terem sido causados danos ou que serão causados danos em certas condições. Estes programas, frequentemente, avisam o utilizador de perigos que não existem, como as mensagens que surgem sobre a formatação do disco rígido (apesar de nenhuma

formatação ter sido feita, na realidade), ou detectam vírus em ficheiros não infectados.

Processos ocultos (Rootkits)

Utilitários usados para esconder actividades maliciosas. Camuflam-se em programas maliciosos para evitarem que os programas Anti-Vírus os detectem. Os rootkits modificam o sistema operativo do computador e alteram as suas funções básicas, para esconder a sua própria existência e acções que o hacker executa no computador infectado.

Outros programas perigosos

Programas criados para activar ataques DoS (recusa de serviço) em servidores remotos, penetrando noutros computadores, e ainda programas que são parte do ambiente de desenvolvimento de programas maliciosos. Estes programas incluem ferramentas de penetração, desenvolvimento de vírus, de procura de vulnerabilidades, programas para descobrir passwords e outros tipos de programas para descobrir recursos de rede ou penetrar num sistema.

Aviso:

A partir daqui, usaremos o termo "vírus" para nos referirmos a programas maliciosos e perigosos. O tipo de programas maliciosos apenas serão enfatizados quando necessário.

CAPÍTULO 2. KASPERSKY ANTI-VIRUS PARA WINDOWS SERVERS 6.0

O Kaspersky Anti-Virus para Windows Servers 6.0 anuncia uma nova geração de produtos de segurança de dados.

2.1. O que há de novo no Kaspersky Anti-Virus para Windows Servers 6.0

Vamos observar as novas funções do Kaspersky Anti-Virus para Windows Servers.

Novas funções de protecção

- A tecnologia de protecção de ficheiros do programa foi alterada: agora pode diminuir a carga sobre o processador central e subsistemas do disco e aumentar a velocidade de verificação de ficheiros. As tecnologias iCheck e iSwift ajudam-no a conseguir isso. Ao funcionar deste modo, a aplicação elimina verificações repetidas de ficheiros.
- O processo de verificação decorre agora, em segundo plano, permitindo que o administrador continue a utilizar o computador. Se houver programas a "competir" pelos recursos do sistema, a verificação de vírus será pausada até que a operação do utilizador seja concluída. A verificação será depois retomada no ponto onde a deixou.
- As áreas críticas do servidor, que podem levar a consequências sérias se estiverem infectadas, têm a sua própria tarefa em separado. Pode configurar esta tarefa para ser executada automaticamente sempre que o sistema se inicia.
- A função de notificação do utilizador (ver 11.8.1 na pág. 144) foi alargada para determinados eventos que surgem durante o funcionamento do computador. Pode seleccionar o método de notificação para cada um destes tipos de eventos: e-mails, notificações sonoras, mensagens de pop-up.

- As novas funções incluem a tecnologia de auto-defesa da aplicação, a protecção contra acesso remoto não-autorizado dos serviços do programa, a protecção dos ficheiros da aplicação em relação ao acesso ou alteração não-autorizados e a protecção das definições do programa através de password.

Novas funções de interface do programa

- A nova interface do Kaspersky Anti-Virus para Windows Servers torna as funções do programa mais simples e fáceis de usar. Também pode mudar a aparência do programa, utilizando o seu próprio grafismo e esquemas de cor.
- Ao utilizar o programa, este fornece, regularmente, dicas: o Kaspersky Anti-Virus para Windows Servers exibe mensagens informativas sobre o nível de protecção, acompanha o seu funcionamento com dicas e inclui uma secção minuciosa de Ajuda.

Novas funções de actualização do programa

- Esta versão do programa estreia o nosso melhorado procedimento de actualização: agora o Kaspersky Anti-Virus verifica, automaticamente, se existem pacotes de actualização na origem de actualização. Quando o Anti-Vírus detecta novas actualizações, transfere-as e instala-as no computador.
- O programa apenas transfere as actualizações que ainda não tiver. Isto reduz, em cerca de 10 vezes, o tráfego de transferência de actualizações.
- As actualizações são transferidas a partir da origem de actualização mais eficiente.
- O programa tem uma função de reversão das actualizações que pode restaurar até à versão anterior das assinaturas se, por exemplo, as assinaturas de ameaças estiverem danificadas ou houver um erro ao copiá-las.
- Foi adicionada uma função para distribuir actualizações numa pasta local para as tornar acessíveis a outros computadores da rede e poupar na largura de banda.

2.2. Como é constituída a Protecção do Kaspersky Anti-Virus para Windows Servers

A protecção do Kaspersky Anti-Virus para Windows Servers inclui:

- Anti-Vírus de Ficheiros (ver 2.2.1 na pág. 17), que monitoriza, em tempo real, o sistema de ficheiros do computador.
- Tarefas de Verificação de Vírus (ver 2.2.2 na pág. 17) que verificam a existência de vírus na memória e sistema de ficheiros do computador, em ficheiros individuais, pastas, discos ou regiões.
- Ferramentas de Suporte (ver 2.2.3 na pág. 18) que dão suporte ao programa e aumentam a sua funcionalidade.

2.2.1. Anti-Vírus de Ficheiros

O servidor é protegido, em tempo real, utilizando o **Anti-Vírus de Ficheiros**.

Um sistema de ficheiros pode conter vírus e outros programas perigosos. Os programas maliciosos podem ser guardados num sistema de ficheiros durante anos, depois de entrarem através de uma disquete ou pela Internet, sem se mostrarem. Mas bastará abrir o ficheiro infectado e o vírus é imediatamente activado.

O *Anti-Vírus de Ficheiros* é a componente que monitoriza o sistema de ficheiros do seu computador. Analisa todos os ficheiros que forem abertos, executados ou guardados no servidor e em todas as unidades de disco ligadas. O Kaspersky Anti-Virus intercepta todas as tentativas para aceder a um ficheiro e verifica o ficheiro quanto à existência de vírus conhecidos. O ficheiro só pode continuar a ser usado se não estiver infectado ou se for tratado pelo Anti-Vírus de Ficheiros com sucesso. Se, por qualquer razão, um ficheiro não puder ser desinfectado, este será apagado, sendo criada uma cópia do mesmo que é guardada na Cópia de Segurança (ver 11.2 na pág. 125) ou sendo movido para a Quarentena (ver 11.1 na pág. 122).

2.2.2. Tarefas de verificação de vírus

Para além do controlo constante de todas as vias potenciais para programas nocivos, através do Anti-Vírus de Ficheiros, é extremamente importante verificar, periodicamente, a existência de vírus no computador. Isto é necessário para

eliminar a possibilidade de disseminação de programas maliciosos que ainda não foram descobertos pelo Anti-Vírus de Ficheiros, porque o nível de segurança é baixo ou por outras razões.

Por defeito, o Kaspersky Anti-Virus para Windows Servers configura as seguintes tarefas de verificação de vírus:

Áreas Críticas

Procura vírus em todas as áreas críticas do computador. Estas incluem: a memória do sistema, programas carregados ao iniciar, sectores de arranque do disco rígido e os directórios do sistema *Microsoft Windows*. A tarefa tenta detectar, rapidamente, os vírus activos no sistema, sem fazer uma verificação completa do computador.

O Meu Computador

Procura vírus no seu computador com uma inspecção minuciosa de todas as unidades de disco, memória e ficheiros.

Objectos de Inicialização

Procura vírus em todos os programas que sejam, automaticamente, carregados ao iniciar, e ainda na memória RAM e nos sectores de arranque dos discos rígidos.

Também tem a opção de criar outras tarefas de procura de vírus e agendá-las.

2.2.3. Ferramentas do programa

O Kaspersky Anti-Virus para Windows Servers inclui uma quantidade de ferramentas de suporte. São concebidas para fornecer suporte ao software em tempo real, expandindo as capacidades do programa e assistindo-o enquanto trabalha.

Actualização

Para estar sempre preparado para apagar um vírus ou outro programa perigoso, o Kaspersky Anti-Virus para Windows Servers precisa de suporte em tempo real. A *Actualização* está concebida precisamente para fazer isso. É responsável por actualizar as assinaturas de ameaças do Kaspersky Anti-Virus para Windows Servers e os módulos do programa.

A função de Distribuição de Actualizações permite-lhe guardar actualizações para a base de dados de assinaturas de ameaças e módulos da aplicação obtidos a partir dos servidores de actualização da Kaspersky Lab e depois torná-las acessíveis a outros computadores da rede para poupar na largura de banda.

Ficheiros de Dados

Durante a sua execução, o Anti-Vírus de Ficheiros e cada tarefa de verificação de vírus e actualização do programa criam um relatório próprio. Os relatórios contêm informação sobre operações concluídas e os seus resultados. Ao usar a função *Relatórios*, estará sempre actualizado sobre o funcionamento de qualquer componente do Kaspersky Anti-Virus para Windows Servers. Se surgirem problemas, poderá enviar os relatórios à Kaspersky Lab para os nossos especialistas poderem estudar a situação em maior detalhe e ajudá-lo com a maior rapidez possível.

O Kaspersky Anti-Virus para Windows Servers envia todos os ficheiros suspeitos de serem perigosos para uma área especial de *Quarentena*. Aqui são guardados encriptados para evitar a infecção do computador. Pode fazer uma verificação de vírus nestes objectos, restaurá-los para os seus locais anteriores, apagá-los ou adicionar, por si próprio, os ficheiros à Quarentena. Após terminar a verificação, todos os ficheiros que se verifique não estarem infectados, são automaticamente restaurados para os seus locais anteriores.

A *Cópia de Segurança* guarda cópias de ficheiros desinfectados e apagados pelo programa. Estas cópias são criadas caso necessite de restaurar os ficheiros ou informação sobre a infecção. As cópias de segurança dos ficheiros são também guardadas de forma encriptada para evitar mais infecções.

Pode restaurar um ficheiro da Cópia de Segurança para o local original e apagar a respectiva cópia.

Suporte

Todos os utilizadores registados do Kaspersky Anti-Virus podem beneficiar do nosso serviço de suporte técnico. Para saber exactamente onde pode obter suporte técnico, use a função *Suporte*.

Utilizando as ligações, pode aceder ao fórum de utilizadores da Kaspersky Lab e procurar perguntas frequentes com respostas que poderão ajudá-lo a resolver o seu problema. Também pode enviar um relatório de erro ou questão sobre o funcionamento do programa para o Suporte Técnico, completando um formulário on-line.

Também poderá aceder ao suporte técnico on-line, e, claro, os nossos funcionários estarão sempre prontos a dar-lhe assistência, por telefone, sobre o Kaspersky Anti-Virus.

2.3. Requisitos de hardware e software de sistema

Para o Kaspersky Anti-Virus funcionar convenientemente, o computador deve obedecer a estes requisitos mínimos:

Requisitos gerais:

- 50 MB de espaço livre no seu disco rígido
- CD-ROM (para instalação do Kaspersky Anti-Virus para Windows Servers 6.0 a partir do CD de instalação)
- Microsoft Internet Explorer 5.5 ou superior (para actualização de assinaturas de ameaças e módulos do programa através da Internet)
- Microsoft Windows Installer 2.0

Sistema operativo:

- Microsoft Windows 2000 Server/Advanced Server Service Pack 4 ou superior, todas as actualizações disponíveis.
- Microsoft Windows NT Server 4.0 Service Pack 6a.
- Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003, todos os Service Packs, todas as actualizações disponíveis.
- Microsoft Windows Server 2003 R2 Standard Edição x64, Microsoft Windows Server 2003 R2 Enterprise Edição x64, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition.

2.4. Pacotes de software

Pode adquirir o Kaspersky Anti-Virus para Windows Servers através dos nossos representantes numa caixa ou através da loja da Internet (por exemplo, www.kaspersky.com, na secção **Loja on-line**).

Se comprar a versão do programa em caixa, esta inclui:

- Um envelope selado com um CD de instalação, contendo os ficheiros de programa
- Uma chave de licença, incluída no pacote de instalação ou numa disquete especial, ou um código de activação colado ao CD de instalação
- Um Manual de Utilizador
- O Contrato de Licença do Utilizador Final (CLUF)

Antes de romper o selo do envelope de instalação do disco, leia cuidadosamente o CLUF.

Se comprar o Kaspersky Anti-Virus para Windows Servers numa loja online, estará a copiar o produto a partir da página da Kaspersky Lab (**Downloads** → **Product Downloads**). Poderá transferir o manual de utilizador na secção **Downloads** → **Documentation**.

Ser-lhe-á enviado uma chave de licença ou um código de activação por e-mail, depois de ter efectuado o pagamento.

O Contrato de Licença do Utilizador Final é um acordo legal entre você e a Kaspersky Lab, que especifica os termos pelos quais poderá usar o software que adquiriu.

Leia o CLUF cuidadosamente.

Se não concordar com os termos do CLUF, poderá devolver o produto embalado ao revendedor onde o comprou e ser reembolsado pela quantidade que pagou pelo programa. Se o fizer, o envelope selado do disco de instalação deve permanecer selado.

Ao abrir o disco selado de instalação, aceitará todos os termos do CLUF.

2.5. Suporte para utilizadores registados

A Kaspersky Lab fornece aos seus utilizadores registados uma série de serviços que tornam o Kaspersky Anti-Virus para Windows Servers mais eficaz.

Após a activação do programa, torna-se num utilizador registado do programa e terá os seguintes serviços disponíveis até a licença expirar:

- Novas versões grátis do programa
- Consultas sobre questões de instalação, configuração e funcionamento do programa, por telefone e e-mail

- Notificações sobre edições do produto da Kaspersky Lab e novos vírus (estes serviços são para utilizadores que subscrevam os mailings de novidades da Kaspersky Lab)

A Kaspersky Lab não dá Suporte Técnico sobre uso e funcionamento do sistema operativo ou outros produtos para além do seu.

CAPÍTULO 3. INSTALAÇÃO DO KASPERSKY ANTI-VIRUS PARA WINDOWS SERVERS 6.0

Existem várias formas para instalar o Kaspersky Anti-Virus 6.0 para Windows Servers:

- Instalação Local: instale a aplicação num único anfitrião. Para executar e concluir a instalação, é necessário ter acesso directo ao anfitrião em questão. Pode efectuar uma instalação local através de um dos seguintes modos:
    - uma instalação interactiva, utilizando o Assistente de Instalação da aplicação (ver 3.1 na pág. 24); este modo requer a inserção de dados pelo utilizador para prosseguir com a instalação;
    - uma instalação não interactiva executada a partir da linha de comandos, utilizando as predefinições e não necessitando de qualquer inserção de dados por parte do utilizador para prosseguir com a instalação (ver 3.3 na pág. 34).
- Instalação Remota: instala a aplicação em computadores em rede, de forma remota a partir de uma estação de trabalho do administrador com a utilização do:
    - Solução de software Kaspersky Administration Kit (ver Guia de Implementação do Kaspersky Administration Kit);
    - Políticas de domínios de grupo Microsoft Windows Server 2000/2003 (ver 3.4 na pág. 35).

Recomenda-se que encerre todas as aplicações em execução antes da instalação do Kaspersky Anti-Virus (inclusive numa instalação remota).

Caso já tenha instalado o Kaspersky Anti-Virus 5.0, este será removido e actualizado para o Kaspersky Anti-Virus 6.0 quando executar o procedimento de instalação (ver 3.5 na pág. 37 para mais detalhes). As actualizações para compilações mais recentes (versões inferiores) no Kaspersky Anti-Virus 6.0 são transparentes.

3.1. Procedimento de instalação usando o Assistente de Instalação

Para instalar o Kaspersky Anti-Virus para Windows Servers no seu computador, abra o ficheiro do Windows Installer no CD de instalação.

> Nota:
>
> Instalar a aplicação com um pacote de instalação transferido da Internet não é diferente da instalação a partir do CD de instalação.

Aparecerá um assistente para a instalação do programa. Cada janela contém um conjunto de botões para navegar ao longo do processo de instalação. Aqui está uma breve explicação das suas funções:

- **Seguinte** – aceita uma acção e avança para a próxima fase da instalação.
- **Anterior** – volta à fase anterior da instalação.
- **Cancelar** – cancela a instalação do produto.
- **Concluir** – completa o procedimento de instalação do programa.

Analisemos, mais detalhadamente, as fases do procedimento de instalação do programa.

Passo 1. Procurar as condições do sistema necessárias para instalar o Kaspersky Anti-Virus para Windows Servers

Antes do programa ser instalado no seu computador, o ficheiro de instalação procura no seu computador o sistema operativo e os pacotes necessários para instalar o Kaspersky Anti-Virus para Windows Servers. Também procura outros programas necessários e verifica se os seus direitos de utilizador lhe permitem instalar o software.

Se alguns destes requisitos falhar, o programa exibirá uma mensagem informando-o desse facto. Antes de instalar o Kaspersky Anti-Virus para Windows Servers, recomenda-se a instalação dos pacotes de serviço necessários através do **Windows Update** e dos programas necessários.

Passo 2. Janela de Boas-vindas da Instalação

Se o seu sistema cumprir todos os requisitos, quando abrir o ficheiro de instalação, aparecerá de imediato uma janela de instalação com informação sobre o início da instalação do Kaspersky Anti-Virus para Windows Servers.

Para prosseguir a instalação, clique no botão **Seguinte**. Pode cancelar a instalação clicando no botão **Cancelar**.

Passo 3. Visualizar o Contrato de Licença do Utilizador Final

A próxima janela contém um Contrato de Licença do Utilizador Final que é acordado entre você e a Kaspersky Lab. Leia tudo com muita atenção, e se concordar com todas as condições do acordo, seleccione **Eu aceito os termos do Contrato de Licença** e clique no botão **Seguinte**. A instalação prosseguirá.

Para cancelar a instalação clique em **Cancelar**.

Passo 4. Seleccionar uma pasta de instalação

O próximo passo da instalação do Kaspersky Anti-Virus para Windows Servers determina onde o programa será instalado no seu computador. O caminho predefinido é o seguinte:

- **<Drive>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 para Windows Servers** – para sistemas 32-bit
- **<Drive>\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus 6.0 para Windows Servers** – para sistemas 64-bit

Poderá especificar uma pasta diferente, clicando no botão **Procurar** e seleccionando-a na janela de selecção da pasta ou inserindo o atalho para a pasta no campo disponível.

Lembre-se que se introduzir, manualmente, o caminho completo para a pasta de instalação, este não deverá exceder os 200 caracteres ou conter caracteres especiais.

Para prosseguir a instalação, clique no botão **Seguinte**.

Passo 5. Utilizar Definições Guardadas na Instalação

Neste passo, é-lhe perguntado para especificar se deseja utilizar as definições de segurança ou assinaturas de ameaças anteriormente guardadas, caso tenham sido guardadas quando removeu do seu servidor uma instalação anterior do Kaspersky Anti-Virus 6.0.

Vamos analisar com maior detalhe sobre como utilizar as opções acima descritas.

Se já teve instalada no seu computador uma outra versão ou compilação do Kaspersky Anti-Virus para Windows Servers e guardou as suas assinaturas de ameaças quando a desinstalou, pode utilizar essas assinaturas na versão actual. Para o fazer, assinale a opção **Assinaturas de ameaças**. As assinaturas de ameaças incluídas com a instalação do programa não serão copiadas para o servidor.

Para utilizar as definições de protecção que configurou e guardou de uma versão anterior, assinale a opção **Definições de protecção**.

Passo 6. Seleccionar o tipo de instalação

Nesta fase, seleccione a quantidade de recursos do programa que deseja instalar no seu computador. Tem duas opções:

Completa. Se seleccionar esta opção, todas as componentes do Kaspersky Anti-Virus para Windows Servers serão instaladas.

Personalizar. Se seleccionar esta opção, terá de seleccionar as componentes do programa que deseja instalar. Para mais informação, veja o Passo 7.

Para seleccionar um tipo de instalação, clique no botão apropriado.

Passo 7. Seleccionar as componentes do programa a instalar

Este passo apenas ocorrerá se seleccionar o tipo de instalação **Personalizar**.

Se seleccionou a instalação **Personalizar**, terá de seleccionar as componentes do Kaspersky Anti-Virus para Windows Servers que deseja instalar. Por defeito, estão seleccionados para instalação o Anti-Vírus de Ficheiros, a componente de verificação de vírus e conector ao Agente de Administração para administração remota através do Kaspersky Administration Kit .

Para seleccionar as componentes que deseja instalar, clique com o botão esquerdo do rato no ícone perto do nome da componente e, no menu de contexto, seleccione **Será instalado no disco rígido local** a partir do menu aberto. Na parte inferior da janela de instalação do programa, encontrará mais informação sobre o tipo de protecção que a componente fornece e sobre o espaço de disco necessário para a instalação.

Se não deseja instalar uma componente, no menu de contexto seleccione **O recurso estará indisponível**.

Após seleccionar as componentes que deseja instalar, clique em **Seguinte**. Para regressar à lista dos programas predefinidos a serem instalados, clique **Repor**.

Passo 8. Procurar outros programas de Anti-Vírus

Nesta fase, o ficheiro de instalação procura outros produtos Anti-Vírus instalados no servidor, incluindo produtos da Kaspersky Lab, que podem causar problemas de compatibilidade com o Kaspersky Anti-Virus para Windows Servers.

Se o ficheiro de instalação detectar algum desses programas, mostrará no ecrã uma lista com os mesmos. O programa perguntará se deseja desinstalá-los antes de prosseguir com a instalação.

Na lista de aplicações Anti-Vírus detectadas, pode seleccionar a desinstalação manual ou automática (apenas os produtos da Kaspersky Lab serão automaticamente apagados).

Para prosseguir com a instalação, clique no botão **Seguinte**.

Passo 9. Concluir a instalação do seu programa

Nesta fase, o programa vai lhe pedir que conclua a instalação do programa no servidor.

Não é aconselhável desmarcar a caixa ☑ **Activar Auto-Defesa antes da instalação** ao instalar, inicialmente, o Kaspersky Anti-Virus 6.0. Ao activar os módulos de protecção, poderá reverter, correctamente, a instalação se ocorrerem erros ao instalar o programa. Se estiver a reinstalar o programa, recomendamos que desmarque esta opção.

Se a aplicação for instalada de forma remota, através do **Windows Remote Desktop**, recomendamos que assinale a caixa ☑ **Activar Auto-Defesa antes da instalação**. Caso contrário, o procedimento de instalação pode não ser concluído ou correctamente concluído.

Se deseja que as exclusões recomendadas da Microsoft para os servidores sejam automaticamente adicionadas à exclusões, assinale a opção ☑ **Excluir da verificação de vírus as áreas recomendadas pela Microsoft**.

Se deseja que a variável de ambiente %Path% seja adicionada ao avp.com após a instalação, assinale a opção **Adicionar caminho à aplicação na variável de ambiente %PATH%**.

Para prosseguir com a instalação, clique no botão **Seguinte**.

Aviso!

Quando estão a ser instaladas as componentes do Kaspersky Anti-Virus que interceptam o tráfego de rede, as actuais ligações de rede são interrompidas. A maioria delas será recuperada após algum tempo.

Passo 10. Concluir o procedimento de instalação

A janela **Concluir Instalação** contém informação sobre como concluir o processo de instalação do Kaspersky Anti-Virus.

Para iniciar o assistente de configuração, clique no botão **Seguinte** (ver 3.2 na pág. 28).

Se a instalação for terminada com sucesso, precisará de reiniciar o seu computador e uma mensagem no ecrã dir-lhe-á isso mesmo.

3.2. Assistente de Configuração

O Assistente de Configuração do Kaspersky Anti-Virus para Windows Servers 6.0 inicia-se no final da instalação do programa. Está concebido para o ajudar a configurar as definições iniciais do programa que estão em conformidade com as características e usos do seu computador.

A interface do Assistente de Configuração está concebida como um Assistente padrão do Windows e consiste numa série de passos que poderá navegar utilizando os botões **Anterior** e **Seguinte** ou concluir utilizando o **botão Concluir**. O botão **Cancelar** parará o Assistente em qualquer momento.

Se parar o assistente de configuração, fechando a janela do assistente, a aplicação não será executada. Cada vez que iniciar a aplicação, o assistente de configuração começará do início até que o procedimento de configuração seja concluído com sucesso.

3.2.1. Utilizar ficheiros guardados da Versão 5.0

Esta janela do assistente aparece depois de concluir o processo de instalação da aplicação em substituição da versão 5.0 do Kaspersky Anti-Virus. Ser-lhe-á pedido para seleccionar quais os dados utilizados pela versão 5.0 que deseja importar para a versão 6.0. Isso pode incluir ficheiros da quarentena ou da cópia de segurança ou ainda definições de protecção.

Para utilizar estes dados na Versão 6.0, seleccione as caixas necessárias.

3.2.2. Activar o programa

Antes de tentar activar o programa, certifique-se de que as definições de data do sistema do computador correspondem à hora e data actuais.

O programa é activado instalando uma chave de licença que o Kaspersky Anti-Virus irá usar para procurar uma licença e determinar a data de validade da mesma.

A chave de licença contém informações sobre o sistema necessárias para o funcionamento de todas as componentes do programa e outra informação:

- Informação de Suporte (quem fornece o apoio e onde obtê-lo)
- Nome, número, e data de validade da sua licença

3.2.2.1. Seleccionar o método de activação do programa

Dependendo se possui uma chave de licença para o Kaspersky Anti-Virus ou se precisa de obter uma a partir do servidor da Kaspersky Lab, existem várias opções para activar o programa:

- **Activar através do código de activação.** Seleccionar esta opção de activação se tiver comprado a versão completa do programa e lhe tiver sido dado um código de activação. Utilizando este código de activação, você obterá um ficheiro de chave que dará acesso a todas as funcionalidades da aplicação durante o prazo efectivo do acordo de licença.
- **Activar versão de avaliação.** Seleccione esta opção de activação se deseja instalar a versão de avaliação do programa antes de decidir comprar a versão comercial. Ser-lhe-á fornecida uma chave gratuita válida durante um período especificado no acordo de licença da versão de avaliação.
- **Aplicar a chave de licença existente.** Active a aplicação, usando um ficheiro da chave de licença do Kaspersky Anti-Virus 6.0.
- **Activar mais tarde.** Se escolher esta opção, saltará a fase de activação. O Kaspersky Anti-Virus para Windows Servers 6.0 será instalado no seu computador e terá acesso a todas as funcionalidades do programa, excepto as actualizações (só poderá actualizar as assinaturas de ameaças quando instalar o programa).

As primeiras duas opções de activação utilizam um servidor de Internet da Kaspersky Lab, o que requer uma ligação à Internet. Antes de activar, certifique-se de que altera as suas definições de rede, se necessário, (ver 10.4.3 na pág. 116) na janela que se abre quando clica em **Definições de LAN**. Para mais

informação detalhada sobre as definições de configuração da rede, contacte o seu administrador de sistema ou o provedor de serviços de Internet.

Se não tiver ligação à Internet quando instalar o programa, pode activar a aplicação mais tarde (ver 11.5 na pág. 137), utilizando a interface da mesma ou pode utilizar o acesso à Internet de outro computador para se registar no site de Suporte Técnico da Kaspersky Lab e obter a chave com o código de activação.

3.2.2.2. Inserir o código de activação

Para activar o programa, você tem que inserir um código de activação. Se tiver comprado o programa através da Internet, receberá o código de activação por e-mail. Se comprou o software numa versão de embalagem, encontrará o código de activação no envelope do CD de instalação.

O código de activação é uma sequência de números e letras separados por traços em quatro secções, cada uma das quais com cinco caracteres, sem espaços. Por exemplo, 11AA1-11AAA-1AA11-1A111. Note que o código tem ser inserido em caracteres latinos.

Introduza a sua informação de contacto na parte inferior da janela: nome completo, endereço de correio electrónico, país e cidade onde reside. Esta informação poderá ser pedida para identificar um utilizador registado, se por exemplo a chave seja perdida ou roubada. Se isso acontecer, a sua informação de contacto permitir-lhe-á obter uma nova chave de licença.

3.2.2.3. Obter um Ficheiro da Chave

O Assistente de Configuração comunica com os servidores da Kaspersky Lab e envia-lhes os seus dados de registo (o código de activação e os dados pessoais), que são verificados no servidor.

Se o código de activação passar a verificação, o Assistente recebe um ficheiro da chave. Se instalar a versão de avaliação do programa, o Assistente de Configuração receberá um ficheiro da chave de avaliação sem código de activação.

O ficheiro obtido será automaticamente instalado para utilizar o programa e verá uma janela “Activação concluída” com informação detalhada sobre a chave actualmente utilizada.

Se o código de activação não passar a inspecção, verá uma mensagem no ecrã. Se tal acontecer, para mais informações, contacte o vendedor do software ao qual comprou o programa, para obter informação.

3.2.2.4. Seleccionar o ficheiro da chave de licença

Se possui um ficheiro da chave de licença para o Kaspersky Anti-Virus para Windows Servers 6.0 , o Assistente perguntar-lhe-á se o deseja instalar. Se quiser, utilize o botão **Procurar** e, na janela de selecção do ficheiro, seleccione o caminho para o ficheiro da chave com a extensão *.key*.

Depois de ter instalado a chave com sucesso, visualizará a informação sobre a licença na parte inferior da janela: nome da pessoa na qual o software está registado, número da licença, tipo de licença (completa, teste beta, demo, etc.), e a data de validade para a chave.

3.2.2.5. Concluir a activação do programa

O Assistente de Configuração informá-lo-á de que o programa foi activado com sucesso. Também disponibilizará informação sobre a chave da licença instalada: nome da pessoa na qual o software está registado, número da licença, tipo de licença (completa, teste beta, demo, etc.), e a data de validade para a chave.

3.2.3. Configurar as definições de actualização

A segurança do seu computador depende directamente da actualização regular das assinaturas de ameaças e dos módulos do programa. Nesta janela, o Assistente de Configuração pede-lhe que seleccione um tipo de actualização do programa e que configure um agendamento para as actualizações.

- **Automaticamente**. O Kaspersky Anti-Virus verifica, em intervalos especificados, se existem actualizações na origem de actualização. As verificações podem ser definidas para serem mais frequentes durante surtos de vírus e menos frequentes quando esses surtos terminam. Quando o Anti-Vírus detecta novas actualizações, transfere-as e instala-as no computador. Esta é a opção predefinida.
- **A cada 2 hora(s)**. As actualizações acontecerão automaticamente segundo o agendamento de actualizações definido. Poderá configurar o agendamento das actualizações, clicando em **Alterar**.
- **Manualmente**. Se escolher esta opção, você mesmo fará as actualizações do programa.

Tenha em atenção que as assinaturas de ameaças e os módulos do programa incluídos no software poderão estar desactualizados na altura em que instalar o programa. É por isso que recomendamos a transferência das últimas

actualizações do programa. Para fazer isso, clique em **Actualizar Agora**. Deste modo, o Kaspersky Anti-Virus para Windows Servers irá transferir as actualizações necessárias a partir dos servidores de actualização e instalá-las-á no seu computador.

Se desejar configurar as actualizações (definir propriedades da rede, seleccionar o recurso a partir do qual as actualizações serão transferidas, configurar a execução de tarefas com uma determinada conta de utilizador ou activar a opção de distribuição de actualizações), clique em **Definições**.

3.2.4. Configurar verificações de vírus agendadas

Uma das tarefas-chave para proteger o seu computador é a verificação de áreas seleccionadas do seu computador, procurando ficheiros maliciosos.

Quando você instala o Kaspersky Anti-Virus para Windows Servers, são criadas três tarefas para verificação de vírus. Nesta janela, o Assistente de Configuração pede-lhe para escolher uma definição de tarefa de verificação.

Objectos de Inicialização

Por defeito, quando o Kaspersky Anti-Virus é iniciado, este verifica, automaticamente, objectos de inicialização. Poderá editar as definições de agendamento noutra janela, clicando em **Alterar**.

Áreas Críticas

Por forma a analisar, automaticamente, as áreas críticas do seu computador (memória do sistema, ficheiros de inicialização, sectores de arranque, pastas de sistema do Windows Server), assinale a caixa apropriada. Poderá configurar o agendamento das actualizações clicando em **Alterar**.

A definição predefinida, para esta verificação automática, está desactivada.

O Meu Computador

Por forma a executar, automaticamente, uma verificação total do seu computador, assinale a caixa apropriada. Poderá configurar o agendamento das actualizações clicando em **Alterar**.

A definição predefinida para executar esta tarefa, de acordo com o agendamento, está desactivada. No entanto, recomendamos uma verificação completa do servidor, imediatamente, após a instalação do programa.

3.2.5. Restringir o acesso ao programa

O Kaspersky Anti-Virus dá-lhe a opção de proteger o programa com uma password, uma vez que várias pessoas poderão usar o mesmo computador e uma vez que os programas maliciosos podem desactivar a protecção. A utilização de uma password pode proteger o programa de tentativas não autorizadas para desactivar a protecção ou alterar as definições.

Para activar a protecção por password, seleccione ☑ **Activar protecção por password** e complete os campos **Password** e **Confirmar password**.

Especifique a área à qual pretende aplicar a protecção por password:

- ◉ **Todas as operações (excepto notificações de objectos perigosos)**. Requer password se o utilizador tentar executar alguma acção com o programa, excepto nas respostas à notificação da detecção de ficheiros perigosos.
- ◉ **Operações seleccionadas:**
  - ☑ **A guardar definições do programa** – Requer password se o utilizador tentar guardar as alterações às definições do programa.
  - ☑ **A sair do programa** – Requer password se o utilizador tentar sair do programa.
  - ☑ **A parar/pausar componentes de protecção ou tarefas de verificação de vírus** – Requer password se o utilizador tentar pausar ou desactivar por completo qualquer componente de protecção ou tarefa de verificação de vírus.

3.2.6. Finalizar o Assistente de Configuração

Na última janela do Assistente, você verá uma mensagem que informa que o programa foi instado e configurado com sucesso. Você pode iniciar a aplicação de imediato, assinalando a opção ☑ **Iniciar o produto**.

Se algo falhou durante a instalação, como por exemplo um problema de incompatibilidade com outras aplicações Anti-Vírus, ser-lhe-á pedido para reiniciar o seu computador.

3.3. Instalar o programa a partir da linha de comandos

Para instalar o Kaspersky Anti-Virus 6.0 para Windows Servers, digite o seguinte na linha de comandos:

```
msiexec /i <package_name>
```

O Assistente de Instalação iniciar-se-á (ver 3.1 na pág. 24). Quando o programa estiver instalado, você tem que reiniciar o computador.

Para instalar a aplicação de forma não interactiva (sem executar o Assistente de Instalação), digite:

```
msiexec /i <package_name> /qn
```

Esta opção implicará que você reinicie, manualmente, a sua máquina depois da instalação estar concluída. Para reiniciar de forma automática a partir da linha de comandos, digite:

```
msiexec /i <package_name> ALLOWREBOOT=1 /qn
```

Por favor, tenha em consideração que a reinicialização automática ocorrerá no modo não interactivo (utilizando a chave /qn).

Para instalar a aplicação com uma password de desinstalação, digite:

`msiexec /i <package_name> KLUNINSTPASSWD=******`, quando efectuar uma instalação interactiva;

`msiexec /i <package_name> KLUNINSTPASSWD=****** /qn`, quando efectuar uma instalação não interactiva sem reiniciar o sistema;

`msiexec /i <package_name> KLUNINSTPASSWD=****** ALLOWREBOOT=1 /qn`, quando efectuar uma instalação não interactiva sem reiniciar o sistema com reinicialização do sistema;

Se instalar o Kaspersky Anti-Virus no modo não interactivo, você pode aceder ao ficheiro *setup.ini*, que contém as definições gerais para a instalação da aplicação (ver A.4 na pág. 194), ao ficheiro de configuração *install.cfg* (ver 13.7 na pág. 182) e ao ficheiro da chave de licença. Tenha em atenção que estes ficheiros devem estar localizados na mesma pasta que o pacote de instalação do Kaspersky Anti-Virus.

3.4. Procedimento para instalar o Objecto de Política de Grupo

Esta função é suportada em computadores com o Microsoft Windows 2000 Server ou superior.

Ao utilizar o **Editor de Objectos de Política de Grupo**, você pode instalar, actualizar e desinstalar o Kaspersky Anti-Virus em estações de trabalho empresariais no âmbito do domínio, sem utilizar o Kaspersky Administration Kit.

3.4.1. Instalar o programa

Para instalar o Kaspersky Anti-Virus:

1. Crie uma pasta partilhada no computador que é o controlador do domínio e copie o pacote de instalação *.msi* do Kaspersky Anti-Virus para essa mesma pasta.

   Também pode copiar o ficheiro *setup.ini*, que contém as definições gerais para a instalação da aplicação (ver A.4 na pág. 194), o ficheiro de configuração *install.cfg* (ver 13.7 na pág. 182) e o ficheiro da chave de licença.

2. Abra o **Editor de Objectos de Política de Grupo** via MMC (para mais informação detalhada sobre a utilização do Objecto de Política de Grupo, consulte a ajuda no Microsoft Windows Server).

3. Crie um novo pacote. Para o fazer, a partir da árvore da consola, seleccione **Objecto de Política de Grupo**/ **Configuração do Computador**/ **Definições do Software**/ **Instalação do Software** e use o comando **Novo**/ **Pacote** a partir do menu de contexto.

   Na janela que se abre, especifique o caminho para a pasta partilhada que contém o programa de instalação Anti-Virus (ver 1). Seleccione **Atribuir** a partir da caixa de diálogo **Seleccionar Método de Instalação** e clique em **OK**.

A política de grupo será implementada em cada estação de trabalho na próxima vez que o computador for registado no domínio. O Kaspersky Anti-Virus será então instalado em todos os computadores.

3.4.2. Actualizar o programa

Para actualizar o Kaspersky Anti-Virus:

1. Copie o pacote de instalação que contém a actualização do Kaspersky Anti-Virus no formato *.msi* para a pasta partilhada.
2. Abra o **Editor de Objectos de Política de Grupo** e crie um novo pacote utilizando os passos acima mencionados.
3. Seleccione o novo pacote e seleccione o comando **Propriedades,** a partir do menu de contexto. Na janela de propriedades de pacote, aceda ao separador **Actualizações** e especifique o pacote que contém o programa de instalação para a versão anterior do Kaspersky Anti-Virus. Para instalar a actualização do Kaspersky Anti-Virus e manter as suas definições de protecção, seleccione uma variante da actualização da versão anterior.

A política de grupo será implementada em cada estação de trabalho na próxima vez que o computador for registado no domínio.

Note que o Kaspersky Anti-Virus em computadores com o Microsoft Windows 2000 Server não pode ser actualizado utilizando o Editor de Objectos de Política de Grupo.

3.4.3. Desinstalar o programa

Para desinstalar o Kaspersky Anti-Virus:

1. Abra o **Editor de Objectos de Política de Grupo**.
2. Para o fazer, a partir da árvore da consola, seleccione **Objecto de Política de Grupo/ Configuração do Computador/ Definições do Software/ Instalação do Software**.

   Seleccione o pacote do Kaspersky Anti-Virus na lista. Abra o menu de contexto e seleccione o comando **Todas as Tarefas/ Remover**.

   Na caixa de diálogo **Remover Software**, seleccione a opção **Desinstalar imediatamente o software dos utilizadores e dos computadores** para que o Kaspersky Anti-Virus seja desinstalado da próxima vez que o computador reiniciar.

3.5. Actualizar da versão 5.0 para a versão 6.0

Se o Kaspersky Anti-Virus 5.0 para Windows File Servers estiver instalado no seu servidor, você pode actualizá-lo para o Kaspersky Anti-Virus 6.0 para Windows Servers.

Depois de iniciar o programa de instalação do Kaspersky Anti-Virus 6.0, ser-lhe-á dada a escolhia de primeiro desinstalar a versão 5.0 já instalada do produto. Quando o programa tiver sido desinstalado, tem de reiniciar o seu computador e depois começará então a instalação da versão 6.0.

Aviso!

Se estiver a instalar o Kaspersky Anti-Virus 6.0 para Windows Servers, a partir de uma pasta de rede protegida por password, sobrepondo uma versão anterior do programa, por favor tome nota do seguinte. Depois de desinstalar a versão 5.0 da aplicação e reiniciar o seu computador, o programa de instalação não lhe permitirá aceder à pasta de rede onde se encontra o pacote de instalação da aplicação. Isto fará com que a instalação do programa seja interrompida. Para instalar o programa correctamente, só deve executar o programa de instalação a partir de uma pasta local.

CAPÍTULO 4. INTERFACE DO PROGRAMA

O Kaspersky Anti-Virus para Windows Servers possui uma interface directa, fácil de utilizar. Este capítulo tratará das suas características básicas:

- Ícone de bandeja do sistema (ver 4.1 na pág. 38)
- Menu de contexto (ver 4.2 na pág. 39)
- Janela principal (ver 4.3 na pág. 40)
- Janela de definições do programa (ver 4.4 na pág. 42)

4.1. Ícone de bandeja do sistema

Logo após a instalação do Kaspersky Anti-Virus para Windows Servers, surgirá um ícone para o mesmo na bandeja do sistema.

O ícone é uma espécie de indicador para as operações do Kaspersky Anti-Virus para Windows Servers. Reflecte o estado da protecção e mostra algumas das funções básicas executadas pelo programa.

Se o ícone estiver activo (a cores), significa que o computador está protegido. Se o ícone estiver inactivo (a preto e branco), significa que a protecção em tempo real está pausada.

O ícone do Kaspersky Anti-Virus para Windows Servers altera-se em função da operação que está a ser executada:

	Está a ser verificado um ficheiro que você ou algum programa está a abrir, a guardar ou a executar.
	As assinaturas de vírus e ameaças do Kaspersky Anti-Virus e os módulos do programa estão a ser actualizados.
	Ocorreu um erro nalguma componente do Kaspersky Anti-Virus.

O ícone também permite o acesso aos elementos centrais da interface do programa: o menu de contexto (ver 4.2 na pág. 39) e a janela principal (ver 4.3 na pág. 40).

Para abrir o menu de contexto, clique sobre o ícone do programa com o botão direito do rato.

Para abrir a janela principal do Kaspersky Anti-Virus para Windows Servers na secção Protecção (este é, por defeito, o primeiro ecrã que aparece quando abre o programa), duas vezes sobre o ícone do programa. Se clicar uma vez, a janela principal abre-se na secção que estava activa da última vez que fechou a janela.

4.2. O menu de contexto

Pode executar tarefas de protecção básicas a partir do menu de contexto (ver Figura 1).

Figura 1. O menu de contexto

O menu do Kaspersky Anti-Virus para Windows Servers contém os seguintes itens:

Verificar o Meu Computador – Inicia uma verificação completa do computador. Serão verificados os ficheiros existentes em todas as unidades, incluindo meios de armazenamento removíveis.

Verificação de vírus... – selecciona objectos e inicia a verificação desses objectos quanto à existência de vírus. Por defeito, a lista contém alguns ficheiros, como por exemplo a memória do sistema, a pasta de inicialização, as bases de dados de e-mail, todas as unidades do seu computador, etc. Pode adicionar objectos à lista, seleccionar ficheiros a serem verificados e iniciar verificações de vírus.

Actualizar – inicia actualizações dos módulos do programa e assinaturas de ameaças e instala-as no seu computador.

Activar... – activa o programa. Tem que activar a sua versão do Kaspersky Anti-Virus para obter o estatuto de utilizador registado que lhe dá acesso à funcionalidade completa da aplicação e ao Suporte Técnico. Este item do menu apenas está disponível se o programa não estiver activado.

Definições... – Permite ver e configurar as definições do Kaspersky Anti-Virus para Windows Servers.

Abrir o Kaspersky Anti-Virus – abre a janela principal do programa (ver 4.3 na pág. 40).

Parar Protecção – activa ou desactiva, temporariamente, o Anti-Vírus de Ficheiros (ver 2.2.1 na pág. 17). Este item do menu não afecta as actualizações do programa ou tarefas de verificação de vírus.

Sair – fecha o Kaspersky Anti-Virus para Windows Servers (quando esta opção é seleccionada, a aplicação será descarregada da memória RAM do computador).

Se estiver a decorrer uma tarefa de pesquisa de vírus, o seu nome será apresentado no menu de contexto com um indicador de progresso percentual. Ao seleccionar a tarefa, você pode aceder à janela de relatório para ver os actuais resultados de desempenho.

4.3. Janela principal do programa

A janela principal do Kaspersky Anti-Virus para Windows Servers (ver Figura 2) pode ser dividida em duas partes:

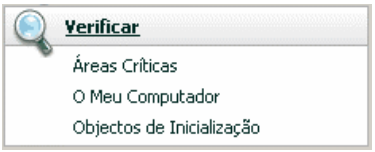
Figura 2. Janela principal do Kaspersky Anti-Virus para Windows Servers

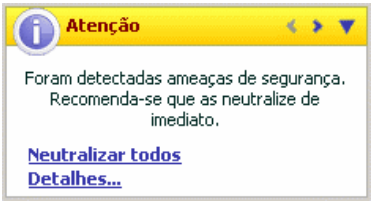
- a parte esquerda da janela, o painel de navegação, guia-o rápida e facilmente até qualquer componente, tarefa de verificação de vírus e de actualização ou funcionalidades do menu de ajuda do programa;

- a parte direita da janela, o painel de informação, contém informação sobre a componente de protecção seleccionada na parte esquerda da janela e apresenta as definições para cada uma delas, oferecendo-lhe ferramentas para executar as nossas verificações de vírus, trabalhar com ficheiros em quarentena e cópias de segurança, gerir chaves de licença, etc.

Depois de seleccionar uma secção na parte esquerda da janela, encontrará informação na parte direita que corresponde à sua selecção.

Examinaremos agora, em maior detalhe, elementos existentes no painel de navegação da janela principal.

Secção da Janela Principal	**Objectivo**
Esta janela serve sobretudo para o informar sobre o estado da protecção do seu computador. A secção **Protecção** está concebida exactamente para isso. 	Aqui encontrará informação geral sobre as operações do Kaspersky Anti-Virus para Windows Servers, permitindo-lhe verificar se tudo está a funcionar correctamente e examinar as estatísticas gerais.
Para verificar o seu computador quanto à existência de ficheiros ou programas maliciosos, utilize a secção **Verificar** na janela principal. 	Esta secção contém uma lista de objectos que pode verificar quanto à existência de vírus. Esta secção contém as tarefas mais comuns e importantes. Estas incluem tarefas de verificação de vírus para áreas críticas, objectos de inicialização e uma verificação completa do computador.
A secção **Serviço** inclui funcionalidades adicionais do Kaspersky Anti-Virus para Windows Servers. 	Aqui poderá actualizar a aplicação, visualizar relatórios sobre as tarefas e componentes em execução e concluídas, trabalhar com objectos em quarentena e da cópia de segurança, rever informação de suporte técnico e gerir chaves de licença.

A secção **Comentários e Dicas** acompanha-o durante a utilização do programa. 	Nesta secção, pode sempre ler dicas sobre como aumentar o nível de protecção do seu servidor. Também vai encontrar comentários acerca do desempenho corrente da aplicação e as suas definições.

Cada elemento do painel de navegação é acompanhado por um menu de contexto especial. Desse modo, o menu contém pontos para o Anti-Vírus de Ficheiros e ferramentas que ajudam o utilizador a configurá-las e geri-las mais rapidamente, e ver relatórios. Existe um item de menu adicional para tarefas de verificação de vírus e de actualização que você pode utilizar para criar a sua própria tarefa com base numa tarefa seleccionada.

Pode mudar a aparência do programa, criando e utilizando os seus próprios gráficos e esquemas de cores.

4.4. Janela de definições do programa

Pode abrir a janela de opções do Kaspersky Anti-Virus para Windows Servers a partir da janela principal (ver 4.3 na pág. 40). Para o fazer, clique em Definições na parte superior dessa janela.

A janela de definições (ver Figura 3) é semelhante à janela principal, em termos de disposição:

- a parte esquerda da janela dá-lhe acesso rápido e fácil às definições do Anti-Vírus de Ficheiros, das tarefas de procura de vírus e de actualização, assim como das ferramentas do programa;
- a parte direita da janela contém uma lista de definições para a componente, tarefa, etc. seleccionada na parte esquerda da janela.

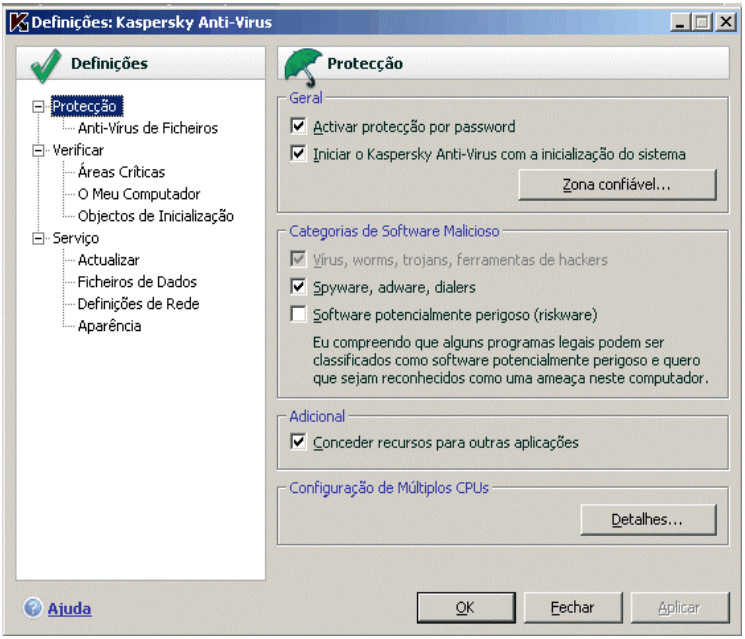


Figura 3. Janela de definições do Kaspersky Anti-Virus para Windows Servers

Quando selecciona uma determinada secção, componente ou tarefa na parte esquerda da janela de definições, a parte direita apresentará as definições básicas para a mesma. Para configurar definições avançadas, pode abrir um segundo e terceiro nível de janelas de definições. Encontrará uma descrição detalhada das opções do programa nas secções aqui presentes.

CAPÍTULO 5. COMO COMEÇAR

Um dos principais objectivos dos especialistas da Kaspersky Lab, ao conceber o Kaspersky Anti-Virus para Windows Servers, foi o de fornecer a configuração óptima para todas as opções do programa. Isso permite que um utilizador, com qualquer nível de conhecimentos informáticos, possa proteger o seu computador logo após a instalação, sem necessitar de despender horas com as definições.

Para a conveniência do utilizador, reunimos as etapas de configuração preliminar numa interface: o Assistente de Configuração Inicial (ver 3.2 na pág. 28) que se inicia assim que o programa é instalado. Ao seguir as instruções do Assistente, você pode activar o programa, configurar definições para as actualizações e verificações de vírus e proteger o acesso ao programa com uma password.

Depois de completar a instalação e iniciar o programa, recomendamos que siga os seguintes passos:

- Verifique o estado actual de protecção (ver 5.1 na pág. 44) para ter a certeza de que o Kaspersky Anti-Virus para Windows Servers está a funcionar com o nível adequado.
- Actualize o programa (ver 5.5 na pág. 52) (se o Assistente de Configuração não o tiver feito automaticamente após a instalação do programa).
- Verifique o computador (ver 5.2 na pág. 50) quanto à existência de vírus.

5.1. Qual o estado da protecção que o meu computador tem?

As informações compostas sobre a protecção do seu computador são fornecidas na janela principal do Kaspersky Anti-Virus na secção **Protecção**. O *actual estado de protecção* do computador e as *estatísticas gerais de funcionamento* do programa são apresentadas aqui.

O **estado de protecção** mostra o actual estado de protecção do seu computador utilizando indicadores especiais (ver 5.1.1 na pág. 45). As estatísticas (ver 5.1.2 na pág. 48) contêm os números para o actual funcionamento do programa.

5.1.1. Indicadores de protecção

O **estado de protecção** é determinado por três indicadores (ver Figura 4), que reflectem o grau de protecção do seu computador naquela altura e que o informam sobre problemas nas definições e desempenho do programa.

Cada indicador pode assumir três possíveis aparências:

– O *indicador é de natureza indicativa*; permite-lhe saber que a protecção do seu computador está no nível adequado e que não foram detectados problemas nas definições e desempenho do programa ou das suas componentes.

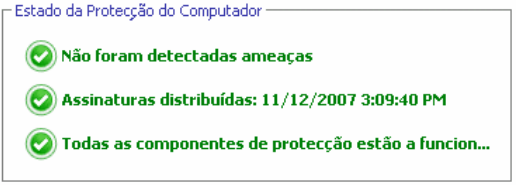

Estado da Protecção do Computador
Não foram detectadas ameaças
Assinaturas distribuídas: 11/12/2007 3:09:40 PM
Todas as componentes de protecção estão a funcion...

Figura 4. Indicadores que reflectem o estado de protecção do programa

– O *indicador direcciona a sua atenção para vários desvios* de desempenho do Kaspersky Anti-Virus para Windows Servers, em relação ao nível de desempenho adequado, o que poderá afectar a segurança da informação. Tenha em atenção as recomendações dos especialistas da Kaspersky Lab. As acções recomendadas são apresentadas como ligações.

– O *indicador reflecte situações críticas* na protecção do seu computador. Siga cuidadosamente as instruções. Elas foram concebidas para uma melhor protecção do seu computador. As acções recomendadas são apresentadas como ligações.

Examinaremos agora, mais detalhadamente, os indicadores de protecção e as situações que cada um deles indica.

O primeiro indicador reflecte a situação com ficheiros e programas maliciosos no seu computador. O indicador assume um dos seguintes valores:

	Não foram detectadas ameaças O Kaspersky Anti-Virus para Windows Servers não detectou qualquer ficheiro ou programa perigoso no seu computador.

	Foram neutralizadas todas as ameaças O Kaspersky Anti-Virus para Windows Servers tratou todos os ficheiros e programas infectados com vírus e apagou aqueles que não podiam ser tratados.
	Foram detectadas ameaças O seu computador está em risco de infecção. O Kaspersky Anti-Virus para Windows Servers detectou programas maliciosos (vírus, Trojans, worms, etc.) que têm que ser neutralizados. Para o fazer, utilize a ligação Neutralizar Todos. Clique na ligação Detalhes para ver informação mais detalhada acerca dos objectos maliciosos.

O segundo indicador reflecte a eficácia da protecção do seu computador naquele momento. O indicador assume um dos seguintes valores:

	Assinaturas distribuídas (data, tempo) A aplicação e as assinaturas de ameaças do Kaspersky Anti-Virus para Windows Servers são as versões mais recentes.
	Assinaturas desactualizadas Os módulos do programa e as assinaturas de ameaças do Kaspersky Anti-Virus para Windows Servers já não são actualizados há uma série de dias. Você está correr o risco de infectar o seu computador com novos programas maliciosos que apareceram desde que actualizou o programa pela última vez. Recomendamos que actualize o Kaspersky Anti-Virus para Windows Servers. Para o fazer, utilize a ligação Actualizar.
	As assinaturas estão parcialmente corrompidas Os ficheiros das assinaturas de ameaça estão parcialmente danificados. Se tal acontecer, recomenda-se que actualize novamente o programa. Se encontrar a mesma mensagem de erro novamente, contacte o Serviço de Suporte Técnico da Kaspersky Lab.
	Por favor, reinicie o seu computador Para que o programa corra correctamente, deverá reiniciar os seu computador. Guarde e feche todos os ficheiros em que estiver a trabalhar e utilize a ligação Reiniciar o computador.

	As actualizações do programa estão desactivadas O serviço de actualização das assinaturas de ameaças e dos módulos do programa está desactivado. Para manter a protecção, em tempo real, recomendamos que active as actualizações.
	As assinaturas estão obsoletas O Kaspersky Anti-Virus para Windows Servers já não é actualizado há algum tempo. Você está a colocar em risco os dados do seu computador. Actualize o programa o mais rapidamente possível. Para o fazer, utilize a ligação Actualizar.
	As assinaturas estão corrompidas Os ficheiros das assinaturas de ameaça estão total ou parcialmente danificados. Se tal acontecer, recomenda-se que actualize novamente o programa. Se encontrar a mesma mensagem de erro novamente, contacte o Serviço de Suporte Técnico da Kaspersky Lab.

O terceiro indicador reflecte o actual estado de funcionamento do programa. O indicador assume um dos seguintes valores:

	Todas as componentes de protecção estão a funcionar O Kaspersky Anti-Virus para Windows Servers está proteger o seu computador em todos os canais através dos quais os programas maliciosos poderão penetrar. Todas as componentes de protecção estão activadas.
	A protecção não está instalada Quando o Kaspersky Anti-Virus para Windows Servers foi instalado, nenhuma das componentes de monitorização foi instalada. Isso significa que apenas pode executar verificações de vírus. Para conseguir máxima segurança, deve instalar as componentes de protecção no seu computador.
	Todas as componentes de protecção estão pausadas A componente de protecção foi pausada. Para restaurar a componente, seleccione **Retomar Protecção** a partir do menu de contexto, clicando no ícone da bandeja do sistema.

	Todas as componentes de protecção estão desactivadas A protecção está completamente desactivada. A componente de protecção não está a funcionar. Para restaurar as componentes, seleccione **Retomar Protecção** a partir do menu de contexto, clicando no ícone da bandeja do sistema.
	Algumas componentes de protecção falharam A componente do Kaspersky Anti-Virus produziram erros internos. Se isso ocorrer, recomenda-se que active a componente ou reinicie o computador (é possível que os controladores da componente tenham que ser registados após terem sido actualizados).

5.1.2. Estado da componente Kaspersky Anti-Virus para Windows Servers

Para descobrir como é que o Kaspersky Anti-Virus para Windows Servers está a proteger o seu sistema de ficheiros ou para visualizar a tarefa de análise de vírus ou o progresso na actualização das assinaturas de ameaça, bastará abrir a secção correspondente da janela principal do programa.

Por exemplo, para visualizar o estado actual do **Anti-Vírus de Ficheiros**, seleccione o Anti-Vírus de Ficheiros na parte esquerda da janela principal. A parte direita da janela exibirá informação completa sobre o funcionamento da componente.

Para o Anti-Vírus de Ficheiros, está dividida na **barra de estado**, a caixa **Estado (Definições** para a análise de vírus e tarefas de actualização) e a caixa **Estatísticas**.

Para o Anti-Vírus de Ficheiros a *barra de estado* aparece da seguinte forma:

- *Anti-Vírus de Ficheiros* : *a executar* – a protecção de ficheiros está activa para o nível seleccionado (ver 7.1 na pág. 74).
- *Anti-Vírus de Ficheiros: pausado* – O Anti-Vírus de Ficheiros está desactivado durante um determinado período de tempo. A componente retomará as operações, automaticamente, depois do período definido ter terminado ou depois de reiniciar o programa. Também pode retomar, manualmente, a protecção de ficheiros, clicando no botão ▶ na barra de estado.

- *Anti-Vírus de Ficheiros: parado* – a componente foi parada pelo utilizador. Pode activar a protecção de ficheiros. Para o fazer, clique no botão ▶ na barra de estado.
- *Anti-Vírus de Ficheiros: não está a funcionar* – Por alguma razão, a protecção de ficheiros não está disponível.
- *Anti-Vírus de Ficheiros: desactivado (erro)* – componente encontrou um erro.

  Se uma componente encontrar um erro, tente reiniciá-la. Se o reinício resultar num erro, reveja o relatório da componente que pode conter a razão para a falha. Se não for capaz de resolver o problema por si só, guarde o relatório da componente num ficheiro, utilizando **Acções** → **Guardar como** e contacte o Suporte Técnico da Kaspersky Lab.

As definições que a componente utiliza no seu funcionamento são apresentadas na secção **Estado**:

- *Anti-Vírus de Ficheiros* – actual estado da componente (em execução, não está a funcionar, pausado, etc.).
- *Nível de segurança* – o conjunto total de parâmetros para o funcionamento da componente, com os quais o programa protege os ficheiros. Por defeito, será seleccionado o nível de segurança **Recomendado**, o qual apenas verifica os objectos no sistema de ficheiros que estão sujeitos a infecção. Por exemplo, ficheiro executáveis (.exe).
- A *acção* tomada quando é detectado um objecto malicioso.

Não existe a caixa de **Estado** para as verificações de vírus ou tarefas de actualização. O nível de segurança, a acção aplicada a programas perigosos para as tarefas de verificação de vírus e o modo de funcionamento para as actualizações estão enumeradas na caixa **Definições**.

A caixa **Estatísticas** contém informação sobre o funcionamento das componentes de protecção, actualizações ou tarefas de verificação de vírus.

5.1.3. Estatísticas de funcionamento do programa

As **estatísticas do programa** podem ser encontradas na caixa **Estatísticas** da secção **Protecção** (ver Figura 5), da janela principal do programa e exibem informação geral sobre a protecção do computador, guardadas desde que instalou o Kaspersky Anti-Virus para Windows Servers.

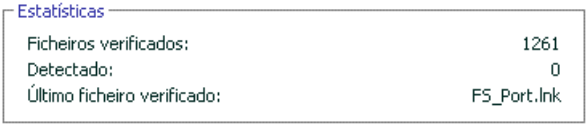


Figura 5. Caixa das estatísticas gerais do programa

Pode clicar com o botão esquerdo do rato em qualquer sítio da caixa para visualizar um relatório com informação detalhada. Os Separadores mostram:

- Informação sobre os objectos encontrados (ver 11.3.2 na pág. 132) e o estado que lhes foi atribuído
- Registo de eventos (ver 11.3.3 na pág. 133)
- Estatísticas gerais de verificação (ver 11.3.4 na pág. 134) para o seu computador
- Definições de funcionamento do programa (ver 11.3.5 na pág. 135)

5.2. Como verificar a existência de vírus no seu servidor

Depois da instalação, o programa informá-lo-á, através de uma mensagem no canto inferior esquerdo da janela do programa, de que o servidor ainda não foi verificado e recomendará que verifique, imediatamente, a existência de vírus no mesmo.

O Kaspersky Anti-Virus inclui uma tarefa predefinida para a verificação de vírus no computador. Esta tarefa está incluída na janela principal do programa na secção **Verificar**.

Após seleccionar a tarefa intitulada **O Meu Computador**, poderá ver as estatísticas da última verificação do computador na parte direita da janela principal e as definições da tarefa: qual o nível de protecção seleccionado e que acções serão tomadas em relação aos objectos perigosos.

Para verificar o seu computador, quanto à existência de programas maliciosos,

1. Abra a janela principal do programa e seleccione a tarefa **O Meu Computador** na secção **Verificar**.
2. Clique no botão **Verificar**.

Como resultado, o programa começará a verificar o seu servidor e os detalhes serão apresentados numa janela especial. Quando clicar no botão **Fechar,** a

janela com informações sobre o progresso da verificação será ocultada. Isso não interromperá a verificação.

5.3. Como verificar as áreas críticas do computador

É extremamente importante garantir a segurança das áreas críticas do seu computador, para assegurar que o mesmo continua a funcionar. Para sua conveniência, programámos antecipadamente uma tarefa de verificação de vírus especificamente para estas áreas. Esta tarefa está incluída na janela principal do programa na secção **Verificar**.

Depois de seleccionar a tarefa intitulada **Áreas Críticas**, poderá ver as estatísticas para a última verificação do computador e as definições da tarefa: que nível de protecção foi seleccionado e quais as acções que são aplicadas em relação a ameaças de segurança. Aqui quais as áreas críticas que pretende verificar e iniciar, de imediato, uma verificação de vírus nas áreas seleccionadas.

Para verificar as áreas críticas do seu computador, quanto à existência de programas maliciosos,

1. Abra a janela principal e seleccione a tarefa **Áreas Críticas** na secção **Verificar**.
2. Clique no botão **Verificar**.

Como resultado, será iniciada uma verificação das áreas seleccionadas e os detalhes serão apresentados numa janela especial. Quando clicar no botão **Fechar,** a janela com informações sobre o progresso da verificação será ocultada. Isso não interromperá a verificação.

5.4. Como verificar a existência de vírus num ficheiro, pasta ou disco

Por vezes é necessário verificar a existência de vírus em objectos individuais e não em todo o computador: por exemplo, um dos discos rígido. Você pode seleccionar um objecto para verificação com as ferramentas padrão do sistema operativo Microsoft Windows Server (por exemplo, na janela do **Explorador** ou na sua **Área de Trabalho**, etc.).

Para analisar um objecto,

Coloque o cursor em cima do nome do ficheiro seleccionado, abra o menu de contexto do Microsoft Windows Server, clicando com o botão direito do rato, e seleccione **Verificar Vírus** (ver Figura 6).

Começará a verificação do objecto seleccionado e os detalhes serão apresentados numa janela especial. Quando clicar no botão **Fechar,** a janela com informações sobre o progresso da verificação será ocultada. Isso não interromperá a verificação.

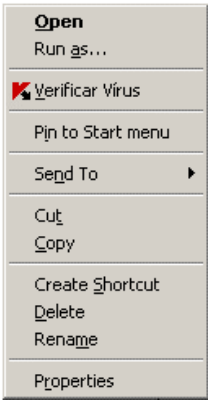


Figura 6. Verificar um ficheiro seleccionado utilizando o menu de contexto padrão do Microsoft Windows Server

5.5. Como actualizar o Programa

A Kaspersky Lab actualiza as assinaturas de ameaças e os módulos internos do Kaspersky Anti-Virus para Windows Servers, utilizando servidores de actualização.

Os *servidores de actualização da Kaspersky Lab* são os sites da Kaspersky Lab onde as actualizações do programa estão armazenadas.

Aviso!

Necessitará de uma ligação à Internet para actualizar o Kaspersky Anti-Virus para Windows Servers.

O Kaspersky Anti-Virus para Windows Servers verifica, automaticamente, a existência de actualizações nos servidores da Kaspersky Lab. Se o servidor tiver as actualizações mais recentes, o Kaspersky Anti-Virus irá transferi-las e instalá-las em modo silencioso.

Para actualizar, manualmente, o Kaspersky Anti-Virus para Windows Servers,

seleccione a componente **Actualização** na secção **Serviço** da janela principal do programa e clique no botão **Actualizar agora!** na parte direita da janela.

Como resultado, o Kaspersky Anti-Virus para Windows Servers começará a actualização. Os detalhes do processo serão apresentados numa janela especial.

5.6. O que fazer se a protecção não estiver a funcionar

Se ocorrerem problemas ou erros no funcionamento do Anti-Vírus de Ficheiros, verifique qual é o estado do mesmo. Se o estado for *não está a funcionar* ou *mau funcionamento*, experimente reiniciar a aplicação.

Se o problema não for resolvido depois de reiniciar o programa, recomendamos que corrija erros possíveis, utilizando a função de restauro da aplicação (**Iniciar → Programas → Kaspersky Anti-Virus 6.0 para Windows Servers → Modificar, reparar ou remover**).

Se o procedimento de restauro da aplicação não ajudar, contacte o Serviço de Suporte Técnico da Kaspersky Lab. Poderá precisar de guardar em ficheiro um relatório sobre o funcionamento da componente ou de toda a aplicação e enviá-lo para a Kaspersky Lab para análise mais aprofundada.

Para guardar o relatório num ficheiro:

1. Seleccione o Anti-Vírus de Ficheiros na secção **Protecção** da janela principal do programa e clique com o botão esquerdo do rato em qualquer parte da secção **Estatísticas**.
2. Clique no botão **Guardar como** e, na janela que se abre, especifique o nome do ficheiro para o relatório de funcionamento da componente.

Para guardar um relatório sobre a inicialização ou estado de todas as componentes do Kaspersky Anti-Virus de uma só vez (Anti-Vírus de Ficheiros, tarefas de verificação de vírus, funcionalidades de suporte:

1. Seleccione a componente na secção **Protecção** da janela principal do programa e clique com o botão esquerdo do rato em qualquer parte da secção **Estatísticas.**

ou

Clique em Todos os relatórios na janela de relatórios para qualquer componente. Deste modo, o Separador **Relatórios** mostrará uma lista de relatórios para todas as componentes do programa.

2. Clique no botão **Guardar como** e, na janela que se abre, especifique o nome do ficheiro para o relatório de funcionamento da componente.

CAPÍTULO 6. SISTEMA DE GESTÃO DA PROTECÇÃO

O Kaspersky Anti-Virus para Windows Servers possibilita-lhe a gestão da segurança do computador com multi-tarefas:

- Activar, desactivar e pausar (ver 6.1 na pág. 55) o programa
- Definir os tipos de programas perigosos (ver 6.2 na pág. 59) em relação aos quais o Kaspersky Anti-Virus para Windows Servers protegerá o seu computador
- Criar uma lista de exclusões (ver 6.3 na pág. 60) da protecção
- Criar a sua própria tarefa de verificação de vírus e actualização (ver 6.4 na pág. 67)
- Configurar agendamento para verificações de vírus (ver 6.5 na pág. 68)
- Configurar definições de produtividade (ver 6.6 na pág. 70) para a protecção do computador

6.1. Parar e Retomar a protecção no seu computador

Por definição, o Kaspersky Anti-Virus arranca e protege o seu computador durante o tempo em que o utilizar. As palavras *Protegido pelo Kaspersky Anti-Virus* no canto superior direito do ecrã informam-no disso. O Anti-Vírus de Ficheiros (ver 2.2.1 na pág. 17) está a funcionar.

Poderá desactivar a protecção fornecida pelo Kaspersky Anti-Virus para Windows Servers.

Aviso!

A Kaspersky Lab recomenda vivamente que **não desactive a protecção**, já que isso poderia levar a uma infecção no seu computador ou à perda de dados.

Note que neste caso a protecção é abordada no contexto do Anti-Vírus de Ficheiros. Desactivar ou pausá-lo não afecta a performance das tarefas de verificação de vírus ou das actualizações do programa.

6.1.1. Pausar a protecção

Pausar a protecção significa desactivar, temporariamente, o Anti-Vírus de Ficheiros.

Para pausar o funcionamento do Kaspersky Anti-Virus para Windows Servers:

1. Seleccione **Parar protecção** no menu de contexto do programa (ver 4.2 na pág. 39).
2. Na janela **Parar protecção** que se abre (ver Figura 7), seleccione o período de tempo a partir do qual você pretende que a protecção seja activada:
   - **Dentro de <intervalo de tempo>** – a protecção será activada após este período de tempo. Para seleccionar um intervalo de tempo, use o menu suspenso.
   - **Na próxima vez que reiniciar o programa** – a protecção será retomada se abrir o programa a partir do Menu Iniciar ou depois de reiniciar o seu computador (desde que o programa esteja definido para se iniciar quando o computador for ligado (ver 6.1.5 na pág. 59).
   - **Apenas a pedido do utilizador** – a protecção estará parada até que você a inicie. Para activar a protecção, seleccione **Retomar Protecção** no menu de contexto do programa.

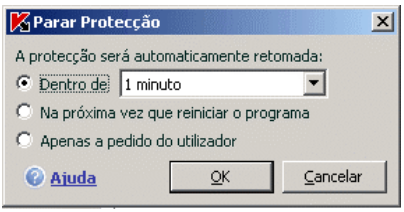


Figura 7. Janela Parar protecção

Dica:

Também pode parar a protecção do seu computador através de um dos seguintes métodos:

- Clique no botão ❚❚ na secção Protecção.
- Seleccione **Sair** no menu de contexto. Neste caso, o programa será descarregado da memória do computador.

Se pausar a protecção, o Anti-Vírus de Ficheiros será pausado. Isto é indicado por:

- Nome inactivo (a cinzento) do Anti-Vírus de Ficheiros na secção **Protecção** da janela principal.
- Ícone da bandeja do sistema inactivo (a cinzento).
- O terceiro indicador de protecção (ver 5.1.1 na pág. 45) do seu computador, que mostra que **Todas as componentes de protecção estão pausadas**.

6.1.2. Desactivar a protecção do servidor

Parar a protecção significa desactivar completamente o Anti-Vírus de Ficheiros. As tarefas de verificação de vírus e actualizações continuarão a funcionar neste modo.

Se a protecção for parada por completo, esta apenas pode ser retomada pelo administrador. O Anti-Vírus de Ficheiros não é automaticamente activado depois de reiniciar o sistema ou o programa. Lembre-se que se o Kaspersky Anti-Virus para Windows Servers estiver, de alguma forma, em conflito com outros programas instalados no seu computador, você pode pausar o Anti-Vírus de Ficheiros ou criar uma lista de exclusões (ver 6.3 na pág. 60).

Para parar, por completo, a protecção:

1. Abra a janela de definições do Kaspersky Anti-Virus e seleccione a secção **Protecção**.
2. Desmarque a opção **Activar protecção**.

Como resultado da desactivação da protecção, o Anti-Vírus de Ficheiros será parado. Isto é indicado através de:

1. Nome inactivo (a cinzento) do Anti-Vírus de Ficheiros na secção **Protecção** da janela principal.
2. Ícone inactivo (cinzento) na bandeja do sistema.
3. O terceiro indicador de protecção (ver 5.1.1 na pág. 45) no seu computador, que mostra que **Todas as componentes de protecção estão desactivadas**.

6.1.3. Pausar / parar a protecção

Existem várias formas de parar o Anti-Vírus de Ficheiros, as verificações de vírus ou as actualizações. No entanto, antes de o fazer, recomendamos que estabeleça a razão pela qual as deseja parar. É provável que consiga resolver o problema de outra forma, por exemplo, alterando o nível de segurança. Se, por exemplo, estiver a trabalhar com uma base de dados que tem a certeza que não contém vírus, pode simplesmente adicionar os seus ficheiros como uma exclusão (ver 6.3 na pág. 60).

Para pausar o Anti-Vírus de Ficheiros, tarefas de verificações de vírus e actualizações:

Seleccione a componente ou tarefa na parte esquerda da janela principal e clique no botão na barra de estado.

O estado da componente/tarefa alterar-se-á para pausado. A componente/tarefa será pausada até que a active, clicando no botão .

Quando pausa uma componente ou tarefa, as estatísticas para a actual sessão do Kaspersky Anti-Virus são guardadas e continuam a ser gravadas depois da componente ser reactivada.

Para parar as componentes ou tarefas de protecção:

Clique no botão na barra de estado. Também pode parar a componente na janela de definições do programa desmarcando a caixa **Activar <nome da componente>** na secção **Geral**.

O estado da componente/tarefa passará então para *desactivado* (parado). A componente ou tarefa ficará parado até que o active clicando no botão . Para as verificações de vírus e actualizações terá de escolher entre as seguintes opções: continuar a tarefa que foi interrompida ou começá-la de novo.

Quando pára a componente ou uma tarefa, todas as estatísticas de trabalhos anteriores são limpas e quando a componente é iniciada, as estatísticas são gravadas por cima, substituindo as anteriores.

6.1.4. Restaurar a protecção no seu computador

Se a dada altura pausou ou desactivou a protecção do seu computador, pode reactivá-la utilizando os seguintes métodos:

- *A partir do menu de contexto*.

Para o fazer, seleccione **Retomar Protecção.**

- *A partir da Janela Principal do Programa.*

  Para o fazer, clique no botão ▶ na barra de estado na secção Protecção na Janela Principal.

O estado da protecção altera-se, de imediato, para *em execução*. O ícone da bandeja do sistema do programa passa a estar activo (a cores). O terceiro indicador de protecção (ver 5.1.1 na pág. 45) também o informará de que **Todas as componentes de protecção estão activadas**.

6.1.5. Encerrar o programa

Se tiver que encerrar o Kaspersky Anti-Virus para Windows Servers, seleccione **Sair** no menu de contexto do programa (ver 4.2 na pág. 39). Isto fechará o programa, deixando o seu computador desprotegido.

Depois de fechar o programa, você pode activar, novamente, a protecção do computador, abrindo o Kaspersky Anti-Virus para Windows Servers (**Iniciar → Programas → Kaspersky Anti-Virus 6.0 para Windows Servers → Kaspersky Anti-Virus 6.0 para Windows Servers**).

Também poderá retomar, automaticamente, a protecção depois de reiniciar o seu sistema operativo. Para activar esta funcionalidade, seleccione a secção **Protecção** na janela de definições do programa e assinale a opção ☑ **Iniciar o Kaspersky Anti-Virus com a inicialização do sistema**.

6.2. Tipos de programas maliciosos a monitorizar

O Kaspersky Anti-Virus para Windows Servers protege o seu computador de vários tipos de programas maliciosos. Sem ter em conta as suas definições, o programa protege sempre o seu computador contra os tipos mais perigosos de programas maliciosos, como vírus, trojans e ferramentas de hackers. Estes programas podem provocar danos significativos no seu computador. Para tornar o seu computador mais seguro, pode aumentar a lista de ameaças que o programa detectará, fazendo-o monitorizar mais tipos de programas perigosos.

Para escolher quais os tipos de programas maliciosos, em relação aos quais o Kaspersky Anti-Virus para Windows Servers o irá proteger, abra a janela de definições da aplicação e seleccione a opção **Ameaças e exclusões** (ver 4.4 na pág. 42).

A caixa **Categorias de Software Malicioso** contém tipos de ameaças (ver 1.1 na pág. 9):

- **Vírus, worms, trojans, ferramentas de hackers**. Este grupo reúne as categorias mais comuns e perigosas de programas maliciosos. Este é o nível de segurança mínimo admissível. De acordo com as recomendações dos especialistas da Kaspersky Lab, o Kaspersky Anti-Virus monitoriza sempre esta categoria de programa malicioso.
- **Spyware, adware, dialers**. Este grupo reúne software potencialmente perigoso que poderia incomodar o utilizador ou causar danos significativos.
- **Software potencialmente perigoso (riskware).** Este grupo inclui programas que não são maliciosos ou perigosos. Contudo, em determinadas circunstâncias, estes podem ser utilizados para causar danos no seu computador.

Os grupos acima listados incluem a totalidade das ameaças que o programa detecta ao verificar objectos.

Se todos os grupos estiverem seleccionados, o Kaspersky Anti-Virus para Windows Servers fornece a protecção Anti-Vírus mais completa possível para o seu computador. Se o segundo e terceiro grupos estiverem desactivados, o programa apenas o protegerá dos programas maliciosos mais comuns. Isto não inclui programas potencialmente perigosos e outros que possam estar instalados no seu computador e que possam causar danos nos seus ficheiros, roubar o seu dinheiro ou consumir o seu tempo.

A Kaspersky Lab aconselha a não desactivar a monitorização do segundo grupo. Se ocorrer uma situação em que o Kaspersky Anti-Virus classifica como potencialmente perigoso um programa que você não considera perigoso, recomendamos que crie uma exclusão para o mesmo (ver 6.3 na pág. 60).

6.3. Criar uma zona confiável

Uma zona *confiável* é uma lista de objectos, criada pelo administrador, que o Kaspersky Anti-Virus para Windows Servers não monitoriza. Ou seja, é um conjunto de programas excluídos da protecção.

O administrador cria uma zona protegida com base nas propriedades dos ficheiros que utiliza e nos programas instalados no seu computador. Você pode precisar de criar uma lista de exclusões se, por exemplo, o Kaspersky Anti-Virus para Windows Servers bloquear o acesso a um objecto ou programa e você tiver a certeza de que o ficheiro ou programa é absolutamente seguro.

Você pode excluir da verificação os ficheiros de determinados formatos, utilizando uma máscara de ficheiro ou excluir uma determinada área (por exemplo, uma pasta ou um programa), processos de programas ou objectos, de

acordo com a classificação da Enciclopédia de Vírus (o estado que o programa atribui aos objectos durante uma verificação).

> Aviso!
>
> Os objectos excluídos não são sujeitos a verificação quando o disco ou pasta onde se encontram é verificado. Contudo, se seleccionar aquele objecto em particular, a regra de exclusão não se aplicará.

Para criar uma lista de exclusões,

1. Abra a janela de definições da aplicação e seleccione a secção **Protecção**.
2. Clique no botão **Zona confiável** na secção **Geral**.

Configure as regras de exclusão para objectos e crie uma lista de aplicações confiáveis na janela que se abre (ver Figura 8).

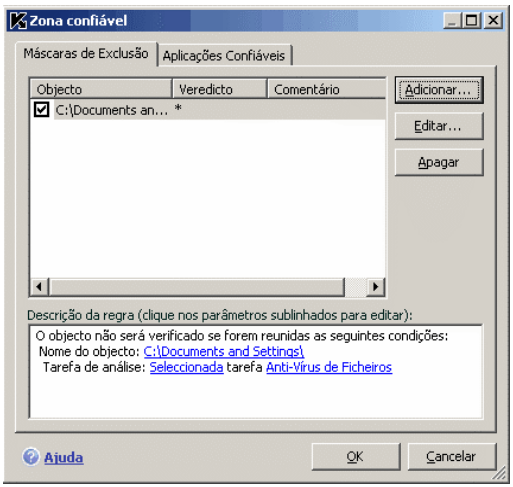


Figura 8. Criar uma zona confiável

6.3.1. Regras de exclusão

As *regras de exclusão* são conjuntos de condições que o Kaspersky Anti-Virus para Windows Servers usa para saber quando não deve verificar um objecto.

Você pode excluir da verificação os ficheiros de determinados formatos, utilizando uma máscara de ficheiro ou excluir uma determinada área (por exemplo, uma pasta ou um programa), processos de programas ou objectos, de acordo com a sua classificação da Enciclopédia de Vírus.

O *veredicto* é o estado que o Kaspersky Anti-Virus atribui a um objecto durante a verificação. Um estado é atribuído com base na classificação de programas maliciosos e potencialmente perigosos encontrados na Enciclopédia de Vírus da Kaspersky Lab.

Os softwares potencialmente perigosos não têm uma função maliciosa, mas podem ser utilizados como componente auxiliar para um código malicioso, uma vez que contém falhas e erros. Esta categoria inclui, por exemplo, programas de administração remota, clientes de IRC, servidores de FTP, utilitários com várias finalidades para parar processos ou escondê-los, keyloggers (registadores de teclas digitadas), macros de password, autodialers (ligações telefónicas automáticas), etc. Tal software não é classificado como vírus, mas pode ser dividido em diversos tipos, tais como Adware, Jokes, Riskware, etc. (para mais informação sobre programas potencialmente perigosos detectados pelo Kaspersky Anti-Virus para Windows Servers, veja a Enciclopédia de Vírus em www.viruslist.com). Como resultado da verificação, tais programas podem ser bloqueados. Visto que muitos deles são largamente utilizados pelos utilizadores, você tem a opção de os excluir da verificação. Para o fazer, tem que adicionar o nome ou máscara da ameaça à zona confiável, utilizando a classificação da Enciclopédia de Vírus.

Por exemplo, no seu trabalho você usa, frequentemente, um programa de Administrador Remoto. Este é um sistema de acesso remoto com o qual você pode trabalhar a partir de um computador remoto. O Kaspersky Anti-Virus para Windows Servers considera este tipo de actividade de aplicação como sendo potencialmente perigosa e poderá bloqueá-la. Para evitar que a aplicação seja bloqueada, você tem que criar uma regra de exclusão que especifica como veredicto: não é vírus:RemoteAdmin.Win32.RAdmin.22.

Quando adiciona uma exclusão, é criada uma regra que o Anti-Vírus de Ficheiros e as tarefas de verificação de vírus podem utilizar mais tarde. Você pode criar regras de exclusão numa janela especial que pode abrir a partir da janela de definições do programa, a partir da janela de aviso da detecção do objecto e a partir da janela de relatório.

*Para adicionar exclusões ao Separador **Máscaras de Exclusão**:*

1. Clicar no botão **Adicionar** no Separador **Máscaras de Exclusão**.
2. Na janela que se abre (ver Figura 9), seleccione o tipo de exclusão na secção **Propriedades**:

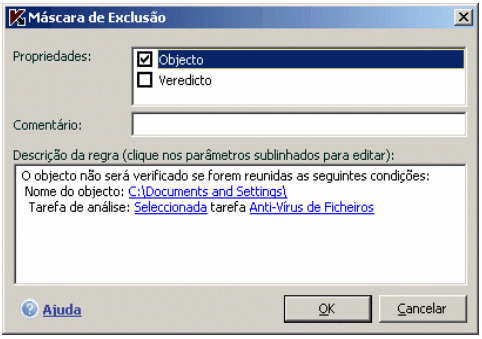


Figura 9. Criar uma máscara de exclusão

☑ **Objecto** – exclui da verificação um determinado objecto, directório ou ficheiros que correspondem a uma determinada máscara.

☑ **Veredicto** – exclui um objecto da verificação, com base no seu estado a partir da classificação da Enciclopédia de Vírus.

Se você assinalar ambas as caixas ao mesmo tempo, será criada uma regra para aquele objecto com um determinado estado, de acordo com a classificação da Enciclopédia de Vírus. Nesse caso, aplicam-se as seguintes regras:

- Se especificar um determinado ficheiro como o **Objecto** e um determinado estado na secção **Veredicto**, o ficheiro especificado apenas será uma exclusão se, durante a verificação, esse ficheiro for classificado como a ameaça seleccionada.
- Se seleccionar uma área ou pasta como o **Objecto** e o estado (ou máscara de veredicto) como o **Veredicto**, então os objectos com aquele estado apenas serão excluídos da verificação naquela área ou pasta.

3. Especificar valores para os tipos de exclusão seleccionados. Para o fazer, na secção **Descrição da regra**, clique com o botão esquerdo do rato na ligação especificar localizada ao lado do tipo de exclusão:
   - Para o tipo **Objecto**, insira o respectivo nome na janela que se abre (isto pode ser um ficheiro, uma pasta em particular ou uma máscara de ficheiro (ver A.2 na pág. 194). Assinale a opção ☑ **Incluir subpastas** para o objecto (ficheiro, máscara de ficheiro, pasta) ser recursivamente excluído da verificação.

- Insira o nome completo da ameaça que pretende excluir da verificação, tal como aparece definido na Enciclopédia de Vírus ou utilize uma máscara para o **Veredicto** (ver A.3 na pág. 194).

  Para alguns objectos das classificações, você pode especificar condições avançadas para a aplicação das regras no campo **Definições avançadas**.

4. Defina quais as componentes do Kaspersky Anti-Virus para Windows Servers que devem utilizar esta regra. Se seleccionar Em qualquer tarefa, esta regra será aplicada a todas as componentes. Se desejar restringir a regra a uma ou diversas componentes, clique na ligação Em qualquer, que se irá alterar para no/na tarefa. Na janela que se abre, assinale as caixas para as componentes às quais você pretende aplicar esta regra de exclusão.

Para criar uma regra de exclusão a partir da janela de notificação de que foi detectado um objecto perigoso:

1. Utilize a ligação Adicionar à zona confiável na janela de notificação.
2. Na janela que se abre, certifique-se de que todas as definições da regra de exclusão estão de acordo com as suas necessidades. O nome do objecto e tipo de ameaça, atribuídos ao objecto, estão automaticamente preenchidos, com base na informação do notificação. Para criar a regra, clique em **OK**.

Para criar uma regra de exclusão a partir da janela de relatório:

1. No relatório, seleccione o objecto que pretende adicionar às exclusões.
2. Abra o menu de contexto e seleccione **Adicionar à Zona Confiável** (ver Figura 10).

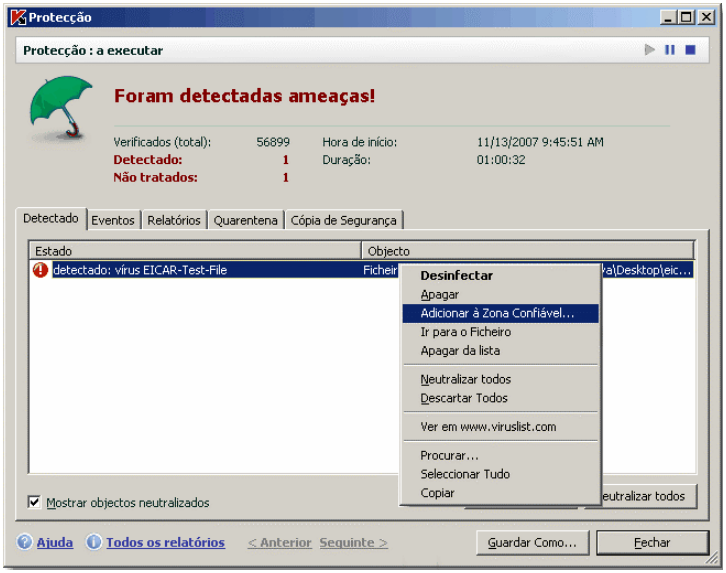


Figura 10. Criar uma regra de exclusão a partir de um relatório

6.3.2. Aplicações confiáveis

O Kaspersky Anti-Virus pode criar uma lista de aplicações confiáveis, cujos ficheiros e actividade de rede não necessitam de ser monitorizados, seja essa actividade suspeita ou de outro tipo.

Por exemplo, você acha que os objectos utilizados pelo Windows Server **Notepad** são seguros e não necessitam de ser verificados. Ou seja, você confia nos processos deste programa. Para excluir da verificação os objectos utilizados por este processo, adicione o **Notepad** à lista de aplicações confiáveis. Contudo, o ficheiro executável e o processo da aplicação confiável serão verificados, quanto à existência de vírus, tal como antes. Para excluir completamente essa aplicação (da tarefa de verificação), você deve usar as regras de exclusão (ver 6.3.1 na pág. 61).

Para além disso, algumas acções classificadas como perigosas são perfeitamente normais para as funcionalidades de alguns programas. Por exemplo, programas que alternam automaticamente a disposição do teclado, tais como o Punto Switcher, normalmente interceptam o texto inserido no seu teclado. Para incorporar esses programas e deixar de monitorizar a sua actividade, recomendamos que os adicione à lista de aplicações confiáveis.

A utilização das exclusões de aplicações confiáveis também pode resolver potenciais conflitos de compatibilidade entre o Kaspersky Anti-Virus para Windows Servers e outras aplicações (por exemplo, o tráfego de rede de outro computador que já foi analisado pela aplicação de Anti-Vírus) e pode incrementar a produtividade do computador.

Por defeito, o Kaspersky Anti-Virus para Windows Servers verifica objectos abertos, executados ou guardados por qualquer processo de programa.

Pode criar uma lista de aplicações confiáveis no Separador especial **Aplicações Confiáveis** (ver Figura 11). Por defeito, a lista de aplicações confiáveis contém uma lista das aplicações que não serão monitorizadas, com base nas recomendações da Kaspersky Lab quando instala o Kaspersky Anti-Virus. Se não confia numa aplicação existente na lista, desmarque a caixa correspondente. Pode editar a lista utilizando os botões do lado direito **Adicionar**, **Editar** e **Apagar**.

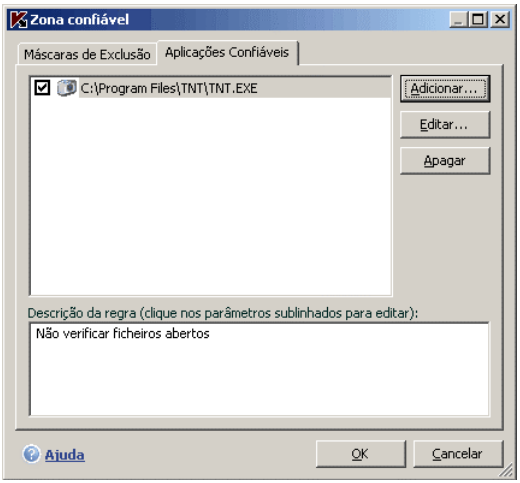


Figura 11. Lista de aplicações confiáveis

Para adicionar um programa à lista de aplicações confiáveis:

1. Clique no botão **Adicionar** no lado direito do separador **Aplicações Confiáveis**.

2. Na janela **Aplicação Confiável** (ver Figura 12) que se abre, seleccione a aplicação utilizando o botão **Procurar**. Abrir-se-á um menu de contexto e, ao clicar em **Procurar**, pode ir para a janela de selecção de ficheiro e seleccionar o atalho para o ficheiro executável ou, clicando **Aplicações,** pode ir para uma lista das aplicações actualmente em funcionamento e seleccionar as necessárias.

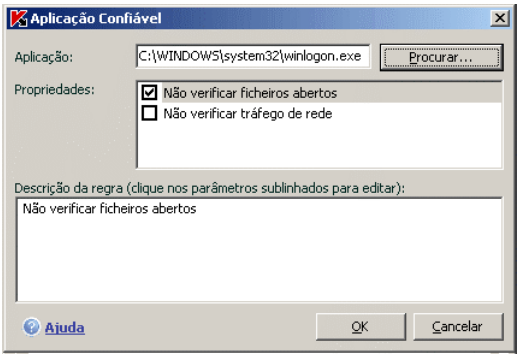


Figura 12. Adicionar uma aplicação à lista de aplicações confiáveis

Quando selecciona um programa, o Kaspersky Anti-Virus para Windows Servers retém os atributos internos do ficheiro executável e usa-os para identificar o programa como confiável durante as verificações.

O caminho do ficheiro é introduzido automaticamente quando selecciona o respectivo nome.

3. Depois, se necessário, especifique quais as acções executadas por este processo que não serão monitorizadas pelo Kaspersky Anti-Virus:

   Não verificar ficheiros abertos – exclui da verificação todos os ficheiros que o processo da aplicação confiável abrir.

6.4. Iniciar tarefas com outro perfil

O Kaspersky Anti-Virus para Windows Servers possui uma funcionalidade que pode iniciar a tarefas de verificação e actualizações com outro perfil de utilizador. Por defeito, esta funcionalidade está desactivada e as tarefas são executadas de acordo com o perfil com a qual você está registado no sistema.

Por exemplo, você poderá precisar de direitos de acesso a um certo ficheiro durante uma verificação. Ao utilizar esta funcionalidade, pode configurar tarefas para funcionarem segundo outro perfil de utilizador que possua os privilégios necessários.

As actualizações do programa podem ser feitas a partir de uma origem à qual você não pode aceder (por exemplo, a pasta de actualização de rede ou direitos de utilizador autorizados para um servidor proxy). Pode utilizar esta funcionalidade para pôr o Actualizador a funcionar com outro perfil que possua esse direitos.

Para configurar uma tarefa de verificação com outro perfil de utilizador:

1. Seleccione o nome da tarefa na secção **Verificar** (para verificações de vírus) ou a secção **Serviço** (para tarefas de actualização) da janela principal e use a ligação Definições para abrir a janela de definições da tarefa.
2. Clique no botão **Personalizar** na janela de definições da tarefa e aceda ao separador **Avançadas** na janela que se abre (ver Figura 13).
3. Para activar esta funcionalidade, seleccione ☑ **Executar esta tarefa como...** Introduza os dados de acesso com os quais você quer iniciar a tarefa: nome de utilizador (conta) e password.

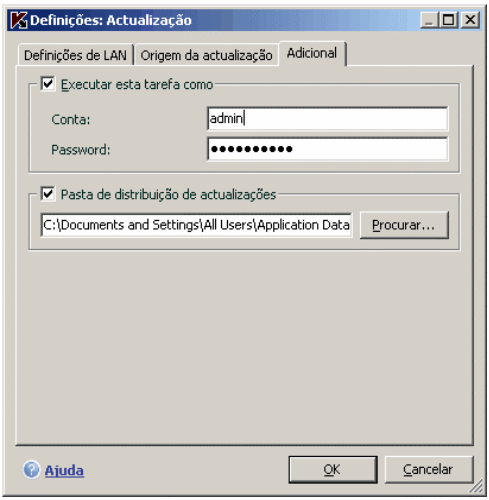


Figura 13. Configurar tarefa de actualização com outro perfil

6.5. Configurar Tarefas e Notificações Agendadas

A configuração de um agendamento é idêntica para as tarefas de verificação de vírus, as actualizações da aplicação e para as notificações de eventos do Kaspersky Anti-Virus.

Por defeito, a definição de agendamento está desligada para as tarefas criadas quando a aplicação é instalada. A única excepção é a verificação dos objectos de inicialização, que é executada sempre que inicia o Kaspersky Anti-Virus. Por

defeito, as actualizações estão configuradas para ocorrerem, automaticamente, à medida que ficarem disponíveis nos servidores de actualização da Kaspersky Lab.

Caso não esteja satisfeito com estas definições, pode reconfigurar o agendamento. Seleccione uma tarefa pelo seu nome por baixo de **Verificar** (para tarefas de verificação de vírus) ou a secção **Serviço** (para actualizações e distribuição de actualizações) e abra a respectiva janela de definições, clicando em Definições.

Para que as tarefas sejam iniciadas de acordo com um horário agendado, assinale a caixa de início automático da tarefa na secção **Modo de Execução**. Pode editar as condições para iniciar a tarefa de verificação na janela **Agendamento** (ver Figura 14), que se abre quando clica em **Alterar**.

Figura 14. Configurar agendamento de tarefas

O primeiro valor a definir é a frequência de um evento (execução da tarefa ou notificação). Seleccione a opção desejada na secção **Frequência** (ver Figura 14). Depois, as definições para a opção seleccionada devem ser especificadas em Definições de Agendamento. Pode seleccionar uma das seguintes opções:

- **A uma hora especificada.** Inicia a tarefa ou envia a notificação no dia e à hora que especificar.
- **Com a inicialização da aplicação**. Executa a tarefa ou envia a notificação sempre que inicia o Kaspersky Anti-Virus. Também pode especificar um tempo de espera para executar a tarefa depois de iniciar a aplicação.
- **Após cada actualização**. A tarefa é executada após cada actualização das bases de dados da aplicação (esta opção apenas se aplica às tarefas de verificação de vírus).
- **Minutos.** O intervalo de tempo entre execuções da tarefa ou notificações será de vários minutos. Defina o intervalo de tempo em minutos nas definições de agendamento. Não deverá exceder os 59 minutos.

- **Horas.** O intervalo entre execuções da tarefa ou notificações será de várias horas. Se escolher esta opção, especifique o intervalo de tempo nas definições de agendamento: **A cada n hora(s)** e defina *N*. Por exemplo, especifique **A cada 1 hora(s)** para executar de hora em hora.
- **Dias.** As tarefas serão iniciadas ou as notificações serão em enviadas com um intervalo de alguns dias. Especifique a duração do intervalo nas definições de agendamento:

  - Seleccione **A cada N dias** e especifique o valor para *N* se deseja ter um intervalo de um determinado número de dias. Seleccione **Todos os dias da semana**, se pretende executar as tarefas diariamente, de Segunda a Sexta-feira.
  - Seleccione **Todos os fins-de-semana** para as tarefas serem executadas apenas aos Sábados e Domingos.

  Use o campo **Hora** para especificar a que hora do dia a tarefa será executada.
- **Semanas**. As tarefas serão iniciadas ou as notificações serão enviadas em certos dias da semana. Se seleccionar esta opção de frequência, assinale com um visto os dias da semana nos quais as tarefas serão executadas com as definições de agendamento. Use o campo **Hora** para definir a hora.
- **Mensalmente**. As tarefas serão iniciadas ou as notificações serão enviadas uma vez por mês à hora especificada.

Se, por alguma razão, uma tarefa não puder ser executada (por exemplo, não estava instalado um programa de e-mail ou computador não estava ligado àquela hora), pode configurar a tarefa para ser automaticamente executada assim que for possível. Assinale a opção ☑ **Executar tarefa se tiver sido ignorada** na janela de agendamento.

6.6. Opções de energia

As verificações de vírus aumentam a carga no processador central e nos subsistemas do disco, diminuindo assim a actividade de outros programas. Por definição, se esta situação acontecer, o programa suspenderá as verificações de vírus e libertará recursos do sistema para as aplicações do utilizador.

No entanto, existem certos programas que podem ser lançados assim que os recursos do processador são libertados e funcionam em segundo plano. Para que as análises de vírus não dependam do funcionamento de tais programas, desmarque a opção ☑ **Conceder recursos para outras aplicações** (ver Figura 15).

Note que esta definição pode ser configurada, individualmente, para cada tarefa de verificação de vírus. Se escolher fazê-lo, a configuração para uma tarefa específica tem uma prioridade mais elevada.

Na janela que se abre quando clica no botão **Configuração de Múltiplos CPUs**, pode atribuir definições para o Kaspersky Anti-Virus para execução a um nível multi-processador. (ver 6.7 na pág. 71).

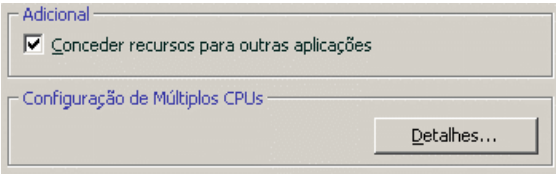


Figura 15. Configurar definições de energia

Para configurar opções de energia:

Seleccione a secção **Protecção** da janela principal do programa e clique na ligação Definições. Configure as opções de energia na caixa **Adicional**.

6.7. Configuração de servidor multi-processador

Nesta janela pode configurar as definições para a produtividade do servidor quando utiliza uma configuração multi-processador.

Número de instâncias do núcleo de Anti-Vírus – número de cópias do núcleo Anti-Virus a serem carregadas quando o Kaspersky Anti-Virus está em execução no servidor. Este número determina o número de processos Anti-Vírus executados ao mesmo tempo.

Quanto mais cópias do motor Anti-Vírus estiverem a ser executadas, mais rapidamente serão processadas as operações Anti-Vírus. Contudo, isto afecta o desempenho global do servidor.

Para além disso, a execução simultânea de vários processos Anti-Vírus no servidor permite que o servidor esteja sempre protegido caso um dos motores apresente um erro.

Para distribuir, de forma automática, os processos Anti-Vírus pelos processadores do servidor, assinale a opção ☑ **Usar controlador especial para gerir processos paralelos**.

Se esta opção estiver desmarcada, você pode regular, manualmente, a carga sobre o servidor. Por exemplo, reservar uma porção dos processadores para o processamento de processos Anti-Vírus e porções das tarefas directas do servidor. Para o fazer, desmarque os processadores dedicados ao servidor na caixa **Processadores utilizados**.

A Kaspersky Lab recomenda que reserve, pelo menos, um processador para as tarefas do servidor quando estiver em execução num servidor multi-processador.

CAPÍTULO 7. PROTECÇÃO ANTI-VÍRUS DO SISTEMA DE FICHEIROS DO SERVIDOR

No Kaspersky Anti-Virus inclui o *Anti-Vírus de Ficheiros,* que protege sistema de ficheiros do computador em relação a um infecção. Este é iniciado quando inicia o seu sistema operativo, é executada na Memória de Acesso Aleatório (RAM) do seu computador e verifica todos os ficheiros abertos, guardados ou executados.

O indicador do funcionamento da componente é apresentado no ícone de bandeja do sistema do Kaspersky Anti-Virus, que apresenta este aspecto sempre que um ficheiro está a ser verificado.

Por defeito, o Anti-Vírus de Ficheiros apenas verifica ficheiros *novos ou modificados*, ou seja, ficheiros que foram adicionados ou modificados desde a verificação anterior. Os ficheiros são verificados de acordo com o seguinte algoritmo:

1. Cada componente intercepta tentativas por parte dos utilizadores ou programas para aceder qualquer ficheiro.
2. O Anti-Vírus de Ficheiros verifica as bases de dados das tecnologias iChecker™ e iSwift™, procurando informação sobre o ficheiro interceptado. Com base na informação recolhida, é tomada uma decisão sobre se verificar ou não o ficheiro.

O processo de verificação inclui os seguintes passos:

1. O ficheiro é analisado em termos da presença de vírus. Os objectos maliciosos são detectados por comparação com as *assinaturas de ameaças* utilizadas pelo programa. As assinaturas contêm descrições de todos os programas maliciosos e ameaças conhecidos até à data e dos métodos para os neutralizar.
2. Depois da análise, estão disponíveis as seguintes opções de comportamento:
    a. Se for detectado um código malicioso no ficheiro, o Anti-Vírus de Ficheiros bloqueia o ficheiro, coloca uma cópia do mesmo na *cópia de segurança* e tenta neutralizar o ficheiro. Se o ficheiro for desinfectado com sucesso, o mesmo passa a estar novamente disponível. Se a desinfecção não for possível, o ficheiro é apagado.

b. Se num ficheiro for detectado um código que parece ser, mas não é efectivamente malicioso, o ficheiro é enviado para a *Quarentena*.

c. Se não for descoberto nenhum código malicioso no ficheiro, o mesmo é imediatamente restaurado.

7.1. Seleccionar um nível de segurança dos ficheiros

O Anti-Vírus de Ficheiros protege os ficheiros que está a utilizar com um dos seguintes níveis (ver Figura 16):

- **Elevado** – o nível com a monitorização mais abrangente dos ficheiros que abre, guarda ou executa.
- **Recomendado** – Os especialistas da Kaspersky Lab recomendam este nível de segurança. Permite verificar as seguintes categorias de objectos:
  - Programas e documentos por conteúdo
  - Objectos novos ou modificados desde a última verificação
  - Objectos OLE incorporados
- **Baixo** – Nível com definições que lhe permitem utilizar, de forma confortável, as aplicações que requerem mais recursos do sistema, uma vez que o conjunto de ficheiros a ser verificado é menor.

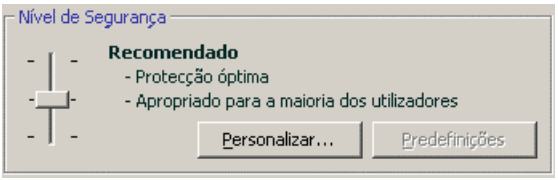


Figura 16. Nível de Segurança do Anti-Vírus de Ficheiros

Por defeito, o Anti-Vírus de Ficheiros está definido no nível **Recomendado**.

Pode aumentar ou baixar o nível de protecção, seleccionando o nível que pretende ou alterando as definições do nível actualmente seleccionado.

Para alterar o nível de segurança:

Ajuste os indicadores. Ao ajustar o nível de segurança, você define o rácio de velocidade de verificação e o total de ficheiros verificados:

quanto menos ficheiros forem sujeitos a verificação em termos de vírus, maior é a velocidade de verificação.

Se nenhum dos níveis de segurança definidos responder às suas necessidades, você pode personalizar as definições de protecção. Para o fazer, seleccione o nível que está mais próximo daquilo que necessita, como ponto de partida, e edite as suas definições. Nesse caso, o nível será estabelecido como **Definições Personalizadas**. Vamos examinar um exemplo de como pode ser útil ter um nível de segurança de ficheiros definido pelo utilizador.

Exemplo:

O trabalho que desenvolve no seu computador implica o uso de um número elevado de tipos de ficheiros diferentes, alguns dos quais podem ser consideravelmente grandes. Você não quer correr o risco de ignorar ficheiros na verificação devido ao seu tamanho ou extensão, mesmo que isto possa afectar a produtividade do seu computador.

Dica para seleccionar um nível de segurança:

Tendo em conta os dados disponíveis, pode-se concluir que existe um risco consideravelmente elevado de se ter uma infecção por um programa malicioso. O tamanho e o tipo de ficheiros a serem tratados é bastante variado e ignorá-los na verificação poderia colocar em risco a informação do seu computador. O requisito básico para a verificação é analisar os ficheiros tratados de acordo com os seus conteúdos, em vez de pela sua extensão.

Recomenda-se que utilize o nível **Recomendado** como o seu nível de segurança básico pré-instalado, inserindo depois as seguintes alterações: remova a restrição sobre o tamanho dos ficheiros a serem verificados e optimize o funcionamento do Anti-Vírus de Ficheiros, limitando a verificação aos ficheiros novos e modificados. Neste caso, será diminuída a carga sobre o computador ao verificar os ficheiros, de forma a que possa utilizar, de forma confortável, as outras aplicações.

Para modificar as definições para um nível de segurança:

Clique no botão **Personalizar** na janela de definições do Anti-Vírus de Ficheiros. Edite as definições do Anti-Vírus de Ficheiros na janela que se abre e clique **OK**.

Desta maneira, será criado um quarto nível de segurança, **Definições Personalizadas**, que contém as definições de protecção que você configurou.

7.2. Configurar o Anti-Vírus de Ficheiros

A configuração determina a forma como o Anti-Vírus de Ficheiros será executado no seu computador. As definições podem ser desagregadas nos seguintes grupos:

- Definições que definem que tipos de objectos que serão verificados (ver 7.2.1 na pág. 76) em termos de vírus
- Definições que definem o âmbito de protecção (ver 7.2.2 na pág. 79)
- Definições que definem a forma como é que o programa responde aos objectos perigosos (ver 7.2.5 na pág. 83)
- Definições adicionais do Anti-Vírus de Ficheiros (ver 7.2.3 na pág. 80)

As secções que se seguem irão examinar, em detalhe, os grupos acima listados

7.2.1. Definir os tipos de ficheiros a serem verificados

Ao especificar os tipos de ficheiros que serão verificados, você estabelece que formatos de ficheiros, que tamanhos e que unidades serão verificadas, em termos de vírus, quando abertos, executados ou guardados.

Para facilitar a configuração, os ficheiros são divididos em dois grupos: *simples e compostos*. Os ficheiros simples não contêm quaisquer objectos. Os ficheiros compostos podem incluir vários objectos, cada um dos quais poderão vários níveis de encadeamento. Existem muitos exemplos: arquivos, ficheiros que contêm macros, tabelas, e-mails com anexos, etc.

Os tipos de ficheiros analisados são definidos na secção **Tipos de ficheiros** (ver Figura 17). Seleccione uma das três opções que se seguem:

- **Verificar todos os ficheiros**. Com esta opção seleccionada, todos os objectos do sistema que estiverem abertos, a funcionar, ou guardados serão analisados sem excepção.
- **Programas e documentos (por conteúdo).** Se seleccionar este grupo de ficheiros, o Anti-Vírus de Ficheiros só analisará ficheiros potencialmente infectados – ficheiros nos quais um vírus se poderia inserir.

> Nota:
>
> Existem alguns formatos de ficheiros que têm um risco relativamente reduzido de possuírem código malicioso inserido neles e, subsequentemente, ser activado. Um exemplo são os ficheiros txt. Por outro lado, existem formatos de ficheiros que contém ou podem conter código executável. Os exemplos são os formatos .exe, .dll, ou .doc. Nesses ficheiros, o risco de inserção e activação de código malicioso é relativamente elevado.

Antes de procurar vírus num ficheiro, é analisado o seu cabeçalho interno no que concerne ao formato de ficheiro (txt, doc, exe, etc.). Se os resultados da verificação demonstrarem que o formato do ficheiro é do tipo dos que não podem ser infectados, esse ficheiro não é verificado em termos de vírus e é imediatamente restaurado para uso. Se o formato de ficheiro permite que o ficheiro seja infectado, esse ficheiro é verificado quanto à existência de vírus.

- **Programas e documentos (por extensão).** Se seleccionar esta opção, o Anti-Vírus de Ficheiros só analisará ficheiros potencialmente infectados, mas o formato do ficheiro será determinado pela extensão. Utilizando a ligação extensão, pode examinar uma lista das extensões de ficheiros que são verificados neste caso (ver A.1 na pág. 190).

> Dica:
>
> Não se esqueça que alguém pode enviar um vírus para o seu computador com uma extensão (.txt por exemplo) que é na realidade um ficheiro executável renomeado como um ficheiro .txt. Se seleccionar a opção **Programas e documentos (por extensão)**, a verificação ignoraria tal ficheiro. Se a opção **Programas e documentos (por conteúdo)** for seleccionada, a extensão é ignorada e a análise dos cabeçalhos dos ficheiros revelará que o ficheiro é um ficheiro .exe. O Anti-Vírus de Ficheiros verificaria o ficheiro quanto à existência de vírus.

Na secção **Produtividade**, poderá especificar que apenas deverão ser analisados, quanto à presença de vírus, os ficheiros novos e aqueles que foram modificados desde a verificação anterior. Este modo de funcionamento reduz, significativamente, o tempo de verificação e aumenta a velocidade de desempenho do programa. Para o fazer, deve escolher a opção **Verificar apenas os ficheiros novos e modificados**.

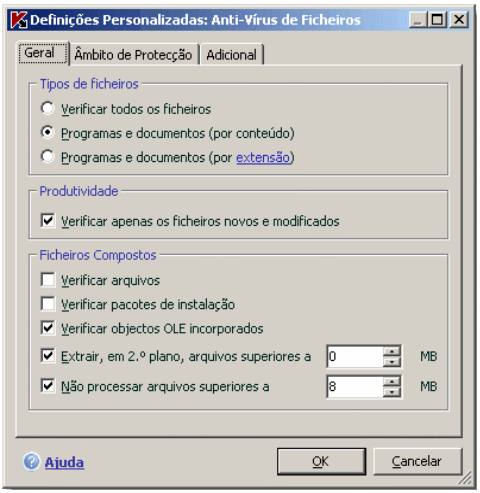


Figura 17. Seleccionar os tipos de ficheiros analisados

Na secção **Ficheiros Compostos**, especifique que ficheiros compostos devem ser analisados:

- **Verificar arquivos** – verifica arquivos .zip, .cab, .rar e .arj.
- **Verificar pacotes de instalação** – analisa arquivos de extracção automática.
- **Verificar Objectos OLE incorporados** – verifica objectos incorporados em ficheiros (por exemplo, folhas de cálculo do Microsoft Office Excel ou uma macro inserida num ficheiro do Microsoft Office Word, anexos de e-mail, etc.).

Para cada tipo de ficheiro composto, você pode seleccionar e verificar todos os ficheiros ou apenas os ficheiros novos. Para o fazer, utilize a ligação que surge antes do nome do objecto. Esta ligação altera-se quando clica com o botão esquerdo do rato sobre a mesma. Se a secção **Optimização** foi definida para apenas verificar ficheiros novos e modificados, você não conseguirá seleccionar o tipo de ficheiros compostos a serem verificados.

Para especificar quais os ficheiros compostos que não deverão ser verificados quanto a vírus, utilize as seguintes definições:

- **Extrair, em 2.º plano, arquivos superiores a... MB.** Se o tamanho de um ficheiro composto exceder esta restrição, o programa irá verificá-lo enquanto um objecto único (analisando o cabeçalho) e irá disponibilizá-lo de novo. Os objectos que esse ficheiro contém serão verificados mais tarde. Se esta caixa não estiver assinalada, o acesso a ficheiros superiores ao tamanho indicado será bloqueado até que os mesmos sejam verificados.

☑ **Não processar arquivos superiores a... MB.** Neste caso, os ficheiros superiores ao tamanho especificado serão ignorados pela verificação.

7.2.2. Definir o âmbito de protecção

Por defeito, o Anti-Vírus de Ficheiros verifica todos os ficheiros quando estes são utilizados, independentemente de onde estiverem armazenados, seja num disco rígido, num CD/DVD-ROM ou num disco flash.

Você pode limitar o âmbito de protecção. Para o fazer:

1. Seleccione o **Anti-Vírus de Ficheiros** na janela principal e aceda à janela de definições de componente clicando em Definições.
2. Clique no botão **Personalizar** e seleccione o Separador **Âmbito de Protecção** (ver Figura 18) na janela que se abre.

O separador apresenta uma lista dos objectos que o Anti-Vírus de Ficheiros irá verificar. Por defeito, a protecção está activada para todos os objectos existentes em discos rígidos, meios removíveis e unidades de rede ligadas ao seu computador. Você pode adicionar objectos à lista ou editar a lista, utilizando os botões **Adicionar**, **Editar** e **Apagar**.

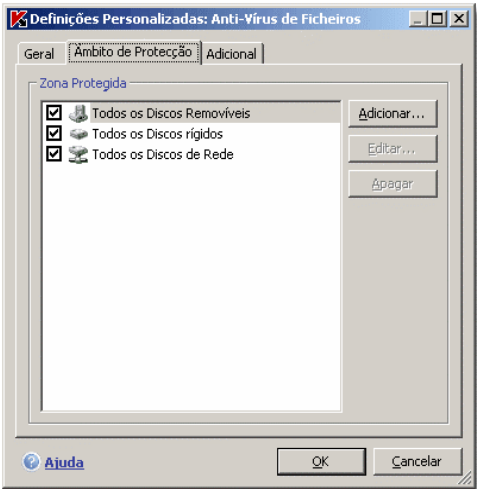


Figura 18. Criar uma zona protegida

Se pretender limitar o conjunto de objectos protegidos, pode fazê-lo utilizando os seguintes métodos:

- Especificar apenas as pastas, unidades e ficheiros que precisam de ser protegidos.
- Criar uma lista de objectos que não necessitam ser protegidos (ver 6.3 na pág. 60).
- Combinar os métodos um e dois – criar um âmbito de protecção a partir do qual alguns objectos são excluídos.

Pode usar máscaras quando adiciona objectos para verificação. Note que apenas pode inserir máscaras com caminhos absolutos para os objectos:

- **C:\dir*.*** ou **C:\dir*** ou **C:\dir** - todos os ficheiros na pasta *C:\dir*
- **C:\dir*.exe** - todos os ficheiros com a extensão *.exe* na pasta *C:\dir*
- **C:\dir*.ex?** – todos os ficheiros com a extensão *.ex?* na pasta *C:\dir*, onde ? pode representar qualquer caractere único
- **C:\dir\teste** – apenas o ficheiro *C:\dir\teste*

Para que a verificação seja executada de forma recursiva, marque a opção ☑ **Incluir subpastas**.

Atenção!

Lembre-se que o Anti-Vírus de Ficheiros irá verificar apenas os ficheiros que estão incluídos no âmbito de protecção que foi criado. Os ficheiros que não estão incluídos nesse âmbito estarão disponíveis para serem utilizados sem verificação. Isto aumenta o risco de uma infecção no seu computador.

7.2.3. Configurar definições avançadas

Nas definições adicionais do Anti-Vírus de Ficheiros pode especificar o modo de verificação do sistema de ficheiros e configurar as condições para pausar, temporariamente, a componente.

Para configurar definições adicionais do Anti-Vírus de Ficheiros:

1. Seleccione o **Anti-Vírus de Ficheiros** na janela principal e acede à janela de definições da componente, clicando na ligação Definições.
2. Clique no botão **Personalizar** e seleccione o separador **Adicional** na janela que se abre (ver Figura 19).

O modo de verificação determina as condições de processamento do Anti-Vírus de Ficheiros. Dispõe das seguintes opções:

- **Modo inteligente**. Este modo destina-se a acelerar o processamento de ficheiros e a devolvê-los ao utilizador. Quando é seleccionado, a decisão

de verificar é tomada com base na análise das operações efectuadas com o ficheiro.

Por exemplo, quando utilizar um ficheiro do Microsoft Office, o Kaspersky Anti-Virus verifica o ficheiro, primeiro, quando este é aberto e, por último, quando este é fechado. Todas as operações intermédias gravadas no ficheiro não são verificadas.

O modo inteligente é a opção predefinida.

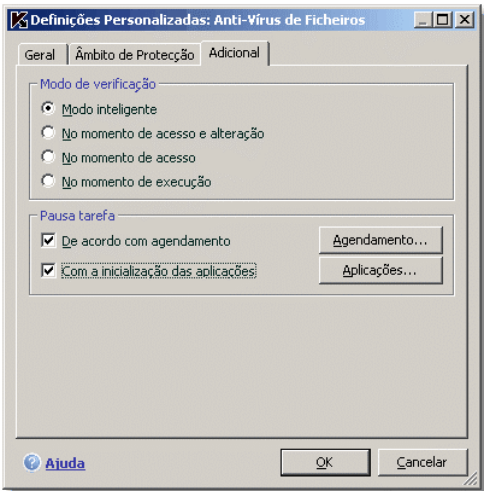


Figura 19. Configurar definições adicionais do Anti-Vírus de Ficheiros

- **No momento de acesso e alteração** – O Anti-Vírus de Ficheiros verifica os ficheiros assim que são abertos ou editados.
- **No momento de acesso** – apenas verifica os ficheiros quando é feita uma tentativa para os abrir.
- **No momento de execução** – apenas verifica dos ficheiros quando é feita uma tentativa para os executar.

Pode precisar de pausar o Anti-Vírus de Ficheiros ao executar tarefas que requerem recursos significativos do sistema operativo. Para reduzir a carga sobre o processador e garantir que o utilizador recupera, rapidamente, o acesso aos ficheiros, recomendamos que configure a componente para se desactivar a uma determinada hora ou enquanto determinados programas estiverem a ser utilizados.

Para pausar a componente, assinale a opção ☑ **De acordo com agendamento** e seleccione o intervalo de tempo para parar e iniciar a componente na janela

que se abre (ver Figura 20) quando clica no botão **Agendamento**. Para o fazer, introduza um valor no formato HH:MM nos campos correspondentes.

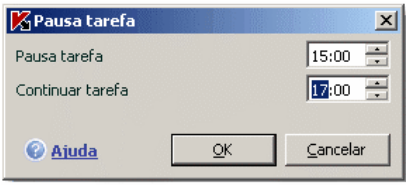


Figura 20. Pausar a componente

Para desactivar a componente quando trabalhar com programas que requeiram recursos significativos, assinale a opção ☑ **Com a inicialização das aplicações** e edite a lista de programas na janela que se abre (ver Figura 21), clicando em **Aplicações**.

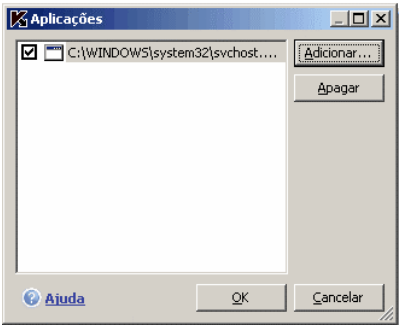


Figura 21. Criar uma lista de aplicações

Para adicionar uma aplicação à lista, utilize o botão **Adicionar**. Abrir-se-á um menu de contexto e, se clicar em **Procurar**, você pode ir para a janela padrão de selecção de ficheiro e especificar o ficheiro executável da aplicação a adicionar. Em alternativa, aceda à lista de aplicações, actualmente, em execução, a partir do item **Aplicações** e seleccione a que desejar.

Para apagar uma aplicação, seleccione-a da lista e clique em **Apagar.**

Pode desactivar, temporariamente, a pausa a efectuar no Anti-Vírus ao utilizar uma aplicação específica. Para o fazer, desmarque o nome da aplicação. Não tem que a apagar da lista.

7.2.4. Restaurar as predefinições do Anti-Vírus de Ficheiros

Ao configurar o Anti-Vírus de Ficheiros, pode sempre voltar às opções de desempenho recomendadas. A Kaspersky Lab considera-as as mais adequadas e combinou-as no nível de segurança **Recomendado**.

Para restaurar as predefinições do Anti-Vírus de Ficheiros:

1. Seleccione o **Anti-Vírus de Ficheiros** na janela principal e aceda à janela de definições da componente, clicando em Definições.
2. Clique no botão **Predefinições** na secção **Nível de Segurança.**

Ao configurar as definições do Anti-Vírus de Ficheiros, se tiver alterado a lista de objectos incluídos na zona protegida, o programa perguntar-lhe-á se deseja guardar aquela lista para uso futuro, quando restaurar as definições iniciais. Para guardar a lista de objectos, assinale a opção **Âmbito de Protecção** na janela que se abre: **Restaurar definições**.

7.2.5. Seleccionar acções para objectos

Quando, ao verificar um ficheiro quanto à existência de vírus, se descobrir que o mesmo está infectado ou se suspeitar que está infectado, as acções subsequentes do Anti-Vírus de Ficheiros dependem do estado dos objectos e da acção seleccionada.

O Anti-Vírus de Ficheiros pode classificar um objecto com um dos seguintes estados:

- Estado de programa malicioso (por exemplo, *vírus, Trojan*) (ver 1.1 na pág. 9).
- *Potencialmente infectado,* quando a verificação não consegue determinar se o objecto está infectado. Isto significa que o código do ficheiro contém uma secção de código que se assemelha a um vírus conhecido mas alterado ou que faz lembrar a estrutura de uma sequência de vírus.

Por defeito, todos os ficheiros infectados são sujeitos a desinfecção e se estiverem potencialmente infectados, então são enviados para a Quarentena.

Para alterar uma acção para um objecto:

Seleccione o **Anti-Vírus de Ficheiros** na janela principal e aceda à janela de definições da componente, clicando em Definições. Todas as acções possíveis são apresentadas nas secções apropriadas (ver Figura 22).

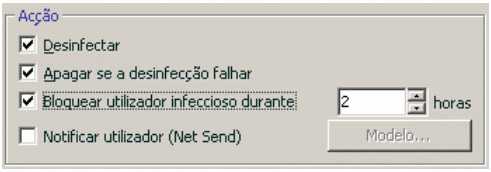


Figura 22. Acções possíveis do Anti-Vírus de Ficheiros em relação a objectos perigosos

Se a acção seleccionada foi	Quando é detectado um objecto perigoso
☑ **Desinfectar** ☐ **Apagar se a desinfecção falhar**	O acesso ao objecto é bloqueado e é feita uma tentativa para o desinfectar. É armazenada uma cópia do objecto na Cópia de Segurança. Se for desinfectado com sucesso, esse objecto é restaurado para utilização regular. Se o objecto não puder ser desinfectado, então é movido para a Quarentena. A informação acerca disto é gravada no relatório. Mais tarde, você pode tentar desinfectar este objecto.
☑ **Desinfectar** ☑ **Apagar se a desinfecção falhar**	O acesso ao objecto é bloqueado e é feita uma tentativa para o desinfectar. É armazenada uma cópia do objecto na Cópia de Segurança. Se for desinfectado com sucesso, esse objecto é restaurado para utilização regular. Se o objecto não puder ser desinfectado, então é apagado.
☐ **Desinfectar** ☑ **Apagar**	O Anti-Vírus de Ficheiros vai bloquear o acesso ao objecto e vai apagá-lo.
☑ **Bloquear utilizador infeccioso durante ... horas**	Bloqueia o acesso ao servidor ou computador a partir do qual foi feita a tentativa para copiar o ficheiro infectado ou potencialmente infectado. Esta acção também pode ser aplicada a acções relacionadas com o processamento do ficheiro (desinfectar

Se a acção seleccionada foi	Quando é detectado um objecto perigoso
	ou eliminar). Note que se o utilizador sair de uma sessão e entrar novamente no sistema, o Kaspersky Anti-Virus considerará isso como uma ligação diferente e a proibição será removida.
☑ **Notificar utilizador (Net Send)**	Notifica o utilizador cujo computador foi usado para uma tentativa para copiar o ficheiro infectado ou potencialmente infectado para o servidor, através do Net Send. Para configurar o modelo de notificação, clique no botão **Modelo** (ver 7.2.6 na pág. 85).

Antes de tentar desinfectar ou apagar um objecto, o Kaspersky Anti-Virus cria uma cópia de segurança e envia-a para a Cópia de Segurança caso o objecto precise de ser restaurado ou surja uma oportunidade de o tratar.

Aviso:

As acções **Bloquear utilizador** e **Net Send** não estão disponíveis se estiver a utilizar a aplicação com o Microsoft Windows NT Server 4.0.

7.2.6. Criar um modelo de notificação

Nesta janela pode formatar o texto para o modelo de notificação para o utilizador cujo computador tentou copiar um ficheiro infectado/potencialmente infectado para o servidor.

O texto da notificação pode conter macros para fornecer informação adicional: o caminho para o objecto perigoso e o nome da ameaça. Para adicionar macros ao texto da notificação, clique em **Macros**.

Para restaurar o texto inicial usado no modelo de notificação, clique no botão **Predefinições**.

7.3. Desinfecção adiada

No Kaspersky Anti-Virus para Windows Servers, o acesso a ficheiros infectados é bloqueado se estes estiverem a ser desinfectados e se apagados, nos casos em que não puderam ser desinfectados ou apagados.

Para recuperar o acesso a objectos bloqueados, primeiro tem que os desinfectar. Para o fazer:

1. Seleccione o **Anti-Vírus de Ficheiros** na janela principal do programa e clique com o botão esquerdo do rato em qualquer parte da caixa **Estatísticas**.
2. Seleccione os ficheiros que lhe interessam no Separador **Detectadas** e clique no botão **Acção** → **Neutralizar Todos**.

Se for desinfectado com sucesso, o ficheiro será devolvido ao utilizador. Se o ficheiro não puder ser tratado, pode *apagá-lo* ou *ignorá-lo*. No último caso, o acesso ao ficheiro será restaurado. No entanto, isto aumenta significativamente o risco de infecção no seu computador. Recomenda-se vivamente a não ignorar os ficheiros maliciosos.

CAPÍTULO 8. VERIFICAÇÃO DE VÍRUS NO SEU COMPUTADOR

O Kaspersky Anti-Virus para Windows Servers pode analisar itens individuais (ficheiros, pastas, discos, mecanismos de Plug and Play), ou o computador inteiro. A análise de vírus impede a disseminação do código malicioso que, por alguma razão, não foi detectado pelo Anti-Vírus de Ficheiros.

O Kaspersky Anti-Virus para Windows Servers inclui as seguintes tarefas de análise predefinidas:

Áreas Críticas

Verifica todas as áreas críticas do computador. Inclui a memória do sistema, programas carregados no arranque, sectores de arranque no disco duro, e os directórios dos sistemas *Windows* e *system32*. A tarefa procura detectar rapidamente vírus activos no sistema sem analisar totalmente o computador.

O Meu Computador

Verifica os vírus no computador com uma inspecção minuciosa de todas as unidades do disco, memória e ficheiros.

Objectos de Inicialização

Verifica todos os programas carregados quando o sistema operativo arranca à procura de vírus.

As definições predefinidas para estas tarefas são as recomendadas. Pode editar estas definições (ver 8.4 na pág. 91) ou criar um agendamento (ver 6.5 na pág. 68) para executar tarefas.

Também pode criar as suas próprias tarefas (ver 8.3 na pág. 90) e criar um agendamento para as mesmas. Por exemplo, pode criar uma tarefa de verificação para as bases de dados de e-mail uma vez por semana ou uma tarefa de verificação de vírus para qualquer pasta **Os Meus Documentos**.

Para além disso, pode analisar qualquer ficheiro à procura de vírus sem criar uma tarefa especial de análise. Pode seleccionar um ficheiro para analisar a partir da interface do Kaspersky Anti-Virus para Windows Servers ou com as ferramentas normalizadas do sistema operativo Windows Server (por exemplo, na janela do programa **Explorer** ou no seu **Ambiente de Trabalho**, etc.).

Pode visualizar uma lista completa de tarefas de análise de vírus para o seu computador, clicando em **Verificar** na parte esquerda da janela principal da aplicação.

8.1. Gerir tarefas de verificação de vírus

Você pode correr uma tarefa de análise de vírus manual ou automaticamente utilizando um agendamento (ver 6.5 na pág. 68).

Para iniciar uma tarefa de análise de vírus manualmente:

Seleccione a caixa junto ao nome da tarefa na secção **Verificar** da janela principal do programa e clique no botão ▶ da barra de estado.

As tarefas actualmente em execução são apresentadas (incluindo tarefas criadas através do Kaspersky Administration Kit) são apresentadas no menu de contexto, clicando com o botão direito do rato no ícone de bandeja do sistema.

Para pausar uma tarefa de verificação de vírus:

Clique no botão ❚❚ na barra de estado. O estado da tarefa alterar-se-á para pausado. Isto suspenderá a verificação até que recomece a tarefa novamente de forma manual ou esta recomeçará, automaticamente, de acordo com o agendamento.

Para parar uma tarefa de verificação de vírus:

Clique no botão ■ da barra de estado. O estado da tarefa alterar-se-á para parado. Isto parará a análise até que recomece a tarefa novamente de forma manual ou esta recomeçará, automaticamente, de acordo com o agendamento. A próxima vez que puser a tarefa a funcionar, o programa perguntar-lhe-á se deseja continuar a tarefa onde ela parou ou recomeçar de novo.

8.2. Criar uma lista de objectos a verificar

Para visualizar uma lista de objectos a serem analisados por uma determinada tarefa, seleccione o nome da tarefa (por exemplo, **O Meu Computador**) na secção **Verificar** na janela principal do programa. Será exibida uma lista dos objectos na parte direita do ecrã por baixo da barra de estado (ver Figura 23).

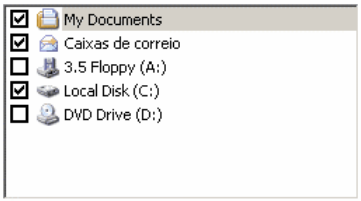


Figura 23. Lista de objectos a analisar

As listas de objectos a analisar estão definidas para as tarefas predefinidas criadas quando instala o programa. Quando você cria as suas tarefas ou selecciona um objecto para uma tarefa de verificação, pode criar uma lista de objectos para essa tarefa.

Você pode adicionar e editar uma lista de verificação de objectos utilizando os botões à direita da lista. Para adicionar um novo objecto de verificação à lista, clique no botão **Adicionar** e, na janela que se abre, seleccione o objecto a ser analisado.

Para conveniência do utilizador, pode adicionar categorias a uma área de verificação, como por exemplo as caixas de e-mail dos utilizadores, a Memória de Acesso Aleatório (RAM), objectos de inicialização, a cópia de segurança do sistema operativo e ficheiros existentes na pasta da Quarentena do Kaspersky Anti-Virus.

Para além disso, quando adiciona uma pasta que contém objectos incorporados a uma área de verificação, você pode editar a recursão. Para o fazer, seleccione um objecto na lista correspondente, abra o respectivo menu de contexto e use a opção **Incluir subpastas**.

Para apagar um objecto, seleccione-o da lista (quando o fizer, o nome do ficheiro será realçado a cinzento) e clique no botão **Apagar**. Pode desactivar temporariamente a verificação de objectos individuais para qualquer tarefa sem os apagar da lista. Para o fazer, desmarque a caixa do objecto que não quer que seja analisado.

Para iniciar uma tarefa de verificação, clique no botão **Verificar** ou seleccione **Iniciar** no menu que se abre quando clicar no botão **Acções**.

Além disso, você também pode seleccionar um ficheiro a ser analisado com as ferramentas standard do sistema operativo Windows Server (por exemplo, na janela do programa Explorer ou no seu Ambiente de Trabalho, etc.) (ver Figura 24). Para o fazer, coloque o cursor sobre o nome do ficheiro seleccionado, abra o menu de contexto do Windows Server, clicando com o botão direito do rato, e seleccione **Verificar Vírus**.

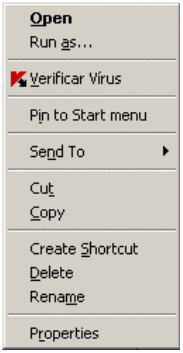


Figura 24. Verificar ficheiros a partir do menu de contexto do Windows

8.3. Criar tarefas de verificação de vírus

Para analisar os vírus no servidor, pode utilizar tarefas incorporadas incluídas no programa e criar as suas próprias tarefas. As novas tarefas são criadas com base nas tarefas de verificação que já existem.

Para criar uma tarefa de verificação nova:

1. Seleccione a tarefa com as definições mais próximas das que necessita na secção **Verificar** da janela principal do programa.
2. Abra o menu de contexto clicando com o botão direito do rato ou clique no botão **Acções** à direita da lista de objectos de verificação e seleccione **Guardar como....**
3. Introduza o nome da nova tarefa na janela que se abre e clique em **OK**. Aparecerá uma tarefa com esse nome na lista de tarefas na secção **Verificar** na janela principal do programa.

Aviso!

Existe um limite no número de tarefas que se pode criar. Esse limite é de quatro tarefas.

A tarefa criada herda todas as propriedades da tarefa em que se baseou. Você precisa de continuar a configurá-la, criando uma lista de objectos de verificação (ver 8.2 na pág. 88), configurando as propriedades que regularão a tarefa (ver 8.4 na pág. 91) e, se necessário, configurar um agendamento (ver 6.5 na pág. 68) para executar a tarefa automaticamente.

Para renomear a tarefa criada:

Seleccione a tarefa na secção **Verificar** na janela principal do programa, clique com o botão direito do rato para abrir o menu de contexto ou clique no botão **Acções**, na parte direita da lista de objectos de verificação, e seleccione **Alterar Nome**.

Introduza o novo nome da tarefa na janela que se abre e clique em **OK**. O nome da tarefa será então alterado na secção **Verificar**.

Para apagar uma tarefa criada:

Seleccione a tarefa na secção **Verificar** na janela principal do programa, clique com o botão direito do rato para abrir o menu de contexto ou clique no botão **Acções,** na parte direita da lista de objectos de verificação, e seleccione **Apagar**.

Confirme a intenção de apagar a tarefa na janela que lhe pede confirmação. A tarefa será então apagada da lista de tarefas na secção **Verificar**.

Aviso!

Só pode renomear e apagar tarefas que você criou.

8.4. Configurar tarefas de verificação de vírus

Os métodos que utiliza para analisar ficheiros no seu computador são determinados pelas propriedades atribuídas a cada tarefa.

Para configurar as definições da tarefa:

Abra a janela principal de definições e seleccione o nome da tarefa na secção **Verificar**.

Pode utilizar a janela de definições para cada tarefa para:

- Seleccionar um nível de segurança com as definições que a tarefa utilizará (ver 8.4.1 na pág. 92)
- Editar as definições avançadas:
    - as definições que definem os tipos de ficheiros que devem ser analisados (ver 8.4.2 na pág. 93)
    - configurar o início da tarefa, utilizando um perfil de utilizador diferente (ver 6.4 na pág. 67)

- configurar definições de verificação avançadas (ver 8.4.5 na pág. 99)

- Restaurar as definições de verificação predefinidas (ver 8.4.3 na pág. 96)
- Seleccionar uma acção que o programa aplicará quando detectar um ficheiro infectado ou potencialmente infectado (ver 8.4.4 na pág. 97)
- Criar um agendamento (ver 6.5 na pág. 68) para executar as tarefas automaticamente.

Além disso, pode configurar as definições globais (ver 8.4.6 na pág. 101) para a execução de todas as tarefas.

As secções que se seguem irão examinar, em detalhe, as definições de tarefa acima listadas.

8.4.1. Seleccionar um nível de segurança

Cada tarefa de verificação de vírus analisa objectos num destes níveis (ver Figura 25):

Elevado – a verificação completa do computador ou dos discos, pastas ou ficheiros. Recomendamos este nível se suspeita que um vírus infectou o seu computador.

Recomendado. Os especialistas da Kaspersky Lab recomendam este nível. A verificação funciona de modo igual ao nível **Elevado**, excepto nos ficheiros de correio electrónico.

Baixo – nível com definições que o deixam utilizar, confortavelmente, as aplicações de recursos intensivos, já que o âmbito dos ficheiros analisados é reduzido.

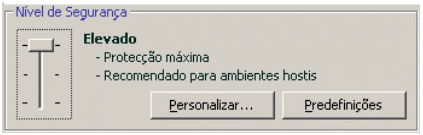


Figura 25. Seleccionar o nível de segurança da verificação de vírus

Por definição, a verificação de ficheiros está configurada no nível **Recomendado**.

Você pode aumentar ou diminuir o nível de segurança de verificação seleccionando o nível que deseja ou alterando as definições para o nível actualmente seleccionado.

Para alterar o nível de segurança:

Ajuste os indicadores. Ao ajustar o nível de segurança, você define o rácio da velocidade de verificação para o número total de ficheiros analisados: quanto menos ficheiros forem analisados, maior a velocidade de verificação.

Se nenhum dos níveis de segurança de ficheiros listados responder às suas necessidades, pode personalizar as definições de verificação. Para o fazer, seleccione o nível que está mais próximo das sua necessidades como ponto de partida e edite as suas definições. Se o fizer, o nível será denominado como **Definições Personalizadas**.

Para modificar as definições para um nível de segurança:

Clique no botão **Personalizar** na janela de definições da tarefa. Edite as definições de verificação na janela que se abrir e clique em **OK**.

Como resultado, será criado um quarto nível de segurança, **Definições Personalizadas** que contém as definições de verificação que você configurou.

8.4.2. Definir os tipos de ficheiros a verificar

Ao especificar os tipos de ficheiros a analisar, você estabelece que tipo de ficheiros, tamanhos e unidades serão analisados quando a tarefa estiver a funcionar.

Os tipos de ficheiros analisados são definidos na secção **Tipos de Ficheiros** (ver Figura 26). Seleccionar uma das três opções:

- **Verificar todos os ficheiros**. Com esta opção, todos os ficheiros serão analisados sem excepção.
- **Programas e documentos (por conteúdo)**. Se seleccionar este grupo de programas, só serão analisados ficheiros potencialmente infectados – ficheiros nos quais um vírus se poderá ter introduzido.

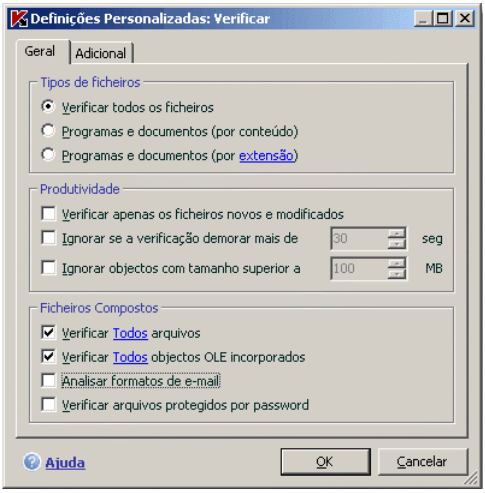


Figura 26. Configurar definições de verificação

> Nota:
>
> Existem alguns formatos de ficheiros que têm um risco relativamente reduzido de possuírem código malicioso inserido neles e, subsequentemente, ser activado. Um exemplo são os ficheiros txt.
>
> Para além disso, existem formatos de ficheiros que contém ou podem conter código executável. Os exemplos são os formatos .exe, .dll, ou .doc. Nesses ficheiros, o risco de inserção e activação de código malicioso é relativamente elevado.

Antes de procurar vírus num ficheiro, o seu cabeçalho interno é analisado para determinar o formato do ficheiro (txt, doc, exe, etc.).

- **Programas e documentos (por extensão).** Neste caso, o programa só analisará ficheiros potencialmente infectados e, ao fazê-lo, o formato do ficheiro será determinado pela extensão. Utilizando a ligação Extensões, pode rever uma lista das extensões de ficheiros que são analisados com esta opção (ver A.1 na pág. 190).

Dica:

Não se esqueça que um vírus num ficheiro com a extensão .txt, poderá ser na realidade um ficheiro executável renomeado como um ficheiro .txt. Se seleccionar a opção **Programas e documentos (por extensão)**, tal ficheiro seria ignorado pela verificação. Se a opção **Programas e documentos (por conteúdo)** for seleccionada, ignorando as extensões, o programa analisará cabeçalhos dos ficheiros, revelando que o ficheiro é, de facto, um ficheiro .exe. Tal ficheiro seria verificado em profundidade, quanto à existência de vírus.

Na secção **Produtividade**, pode especificar que apenas serão verificados os ficheiros novos e aqueles que foram modificados desde a última verificação. Este modo reduz, notavelmente, o tempo de análise e aumenta a velocidade de desempenho do programa. Para o fazer, deve seleccionar a opção **Verificar apenas os ficheiros novos e modificados**. Este modo estende-se aos ficheiros simples e compostos.

Na secção **Produtividade,** também pode estabelecer limites de tempo e de tamanho para os ficheiro a verificar.

- **Ignorar se a verificação demorar mais de ... segundos.** Seleccione esta opção e introduza o tempo de verificação máximo para um ficheiro. Desse modo, se este tempo for excedido, este ficheiro será removido da fila da verificação.
- **Ignorar objectos com tamanho superior a ... MB**. Seleccione esta opção e introduza o tamanho máximo para um ficheiro. Desse modo, se o tamanho for excedido, este ficheiro será removido da fila da verificação.

Na secção **Ficheiros Compostos**, especifique que ficheiros compostos devem ser verificados:

- **Verificar Todos arquivos** – verifica os arquivos .rar, .arj, .zip, .cab. .lha, .jar, e .ice.

Aviso!

O Kaspersky Anti-Virus não apaga automaticamente formatos de ficheiros comprimidos que não suporta (por exemplo, .ha, .uue, .tar), mesmo se tiver seleccionado a opção para tratar automaticamente ou eliminar se os objectos não puderem ser tratados.

Para apagar esses ficheiros comprimidos, clique na ligação Apagar arquivos na janela de aviso sobre a detecção do objecto perigoso. O ecrã apresenta esta mensagem quando é seleccionada a opção **Perguntar o que fazer durante a verificação/Perguntar ao que fazer quando a verificação for concluída** (ver 8.4.4 na pág. 97). Também pode apagar manualmente os ficheiros infectados.

☑ **Verificar Todos objectos OLE incorporados** – verifica os objectos incorporados nos ficheiros (por exemplo, as folhas de cálculo do Excel ou uma macro incorporada num ficheiro do Microsoft Word, anexos de correio electrónico, etc.).

Para cada tipo de ficheiros compostos, pode seleccionar e analisar todos os ficheiros ou só os novos. Para o fazer, utilize a ligação junto ao nome dos ficheiros. Isto alterará o seu valor quando clicar nela com o botão esquerdo do rato. Se a secção **Produtividade** foi configurada para só analisar ficheiros novos ou modificados, você apenas poderá seleccionar o tipo de ficheiros compostos a serem verificados.

☑ **Analisar formatos de e-mail** – analisa ficheiros de e-mails e bases de dados de e-mails. Se esta caixa não estiver seleccionada, os ficheiro de formato e-mail serão analisados como ficheiros binários (sem dissecar o formato) e se o ficheiro não estiver infectado e o parâmetro **Verificar todos os ficheiros** estiver seleccionado, a informação será gravada no relatório com o estado *OK*. Se as definições de verificação de ficheiros foram seleccionadas por tipo e extensão, o ficheiro será ignorado, com o veredicto *excluído por tipo*.

Repare nestes pontos de verificação de bases de dados de correio electrónico protegidas por palavra-passe:

- O Kaspersky Anti-Virus para Windows Servers detecta código malicioso na base de dados do Microsoft Office Outlook 2000 mas não o trata;
- O Kaspersky Anti-Virus para Windows Servers não suporta análises de código malicioso nas bases de dados protegidas do Microsoft Office Outlook 2003.

☑ **Verificar arquivos protegidos por password** – verifica os arquivos protegidos por password. Com esta funcionalidade, uma janela pedirá uma password perante os ficheiros arquivados analisados. Se esta caixa não estiver seleccionada, os arquivos protegidos por password não serão analisados.

8.4.3. Restaurar as definições de verificação predefinidas

Ao configurar as definições das tarefas de verificação, você pode sempre retornar às definições recomendadas. A Kaspersky Lab considera-as as mais adequadas e combinou-as no nível de segurança **Recomendado**.

Para restaurar as predefinições das verificações de vírus:

1. Seleccione o nome da tarefa na secção **Verificar** da janela principal e use a ligação Definições para abrir a janela de definições da tarefa.
2. Clique no botão **Predefinições** na secção **Nível de Segurança**.

8.4.4. Seleccionar acções para objectos

Quando, ao verificar um ficheiro quanto à existência de vírus, se descobrir que o mesmo está infectado ou se suspeitar que está infectado, as acções subsequentes do programa dependem do estado dos objectos e da acção seleccionada.

Uma das seguintes classificações podem ser atribuídas a um ficheiro depois da verificação:

- Programa malicioso (por exemplo, *vírus, Trojan*).
- *Potencialmente infectado,* quando a verificação não consegue determinar se o objecto está infectado. É provável que o programa tenha detectado uma sequência de código no ficheiro resultante de um vírus desconhecido ou código modificado de um vírus conhecido.

Por defeito, todos os ficheiros infectados são sujeitos à desinfecção e, se estiverem potencialmente infectados, são enviados para a Quarentena.

Para editar uma acção para um objecto:

seleccione o nome da tarefa na secção **Verificar** da janela principal do programa e utilize a ligação Definições para abrir a janela de definições da tarefa. Todas as acções possíveis são apresentadas nas secções apropriadas (ver Figura 27).

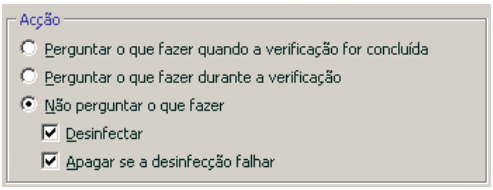

Acção
Perguntar o que fazer quando a verificação for concluída
Perguntar o que fazer durante a verificação
Não perguntar o que fazer
Desinfectar
Apagar se a desinfecção falhar

Figura 27. Seleccionar acções para ficheiros perigosos

Se a acção seleccionada foi	Quando detecta um objecto malicioso ou potencialmente infectado
◉ **Perguntar o que fazer quando a verificação for concluída**	O programa não processa os ficheiros antes do fim da verificação. Quando a verificação está completa, a janela das estatísticas aparecerá com uma lista de objectos detectados um após o outro, solicitando uma acção para cada um dos objectos.
◉ **Perguntar o que fazer durante a verificação**	O programa emitirá uma mensagem de aviso que contém informação sobre o código malicioso que infectou (infectou potencialmente) o ficheiro e dá-lhe a escolher uma das seguintes acções.
◉ **Não perguntar o que fazer**	O programa grava informação sobre os objectos detectados no relatório, sem os ter processado ou emitir notificação. Não recomendamos que utilize esta funcionalidade, já que os objectos infectados e potencialmente infectados permanecem no servidor e é, praticamente impossível, evitar a infecção.
◉ **Não perguntar o que fazer** ☑ **Desinfectar**	O programa tenta tratar o objecto detectado sem pedir confirmação. Se o ficheiro puder ser desinfectado, o mesmo é movido para a Quarentena para ser desinfectado mais tarde. Se o programa não conseguir desinfectar o objecto, o acesso ao mesmo é bloqueado.
◉ **Não perguntar o que fazer** ☑ **Desinfectar** ☑ **Apagar se a desinfecção falhar**	O programa tenta tratar o ficheiro detectado sem pedir confirmação. Se o ficheiro não puder ser desinfectado, o mesmo é apagado. É guardada uma cópia do mesmo na Cópia de Segurança.

Se a acção seleccionada foi	Quando detecta um objecto malicioso ou potencialmente infectado
◉ **Não perguntar o que fazer** ☐ **Desinfectar** ☑ **Apagar**	O programa apaga o ficheiro automaticamente

Ao desinfectar ou apagar um objecto, o Kaspersky Anti-Virus cria uma cópia de segurança e envia-a para a Cópia de Segurança (ver 12.2 na pág. 159) antes de tentar tratar o objecto o apagá-lo, caso o objecto precise de ser restaurado ou surja uma oportunidade de o tratar.

Quando o estado é *potencialmente infectado*, o objecto é movido para a Quarentena sem tentar desinfectá-lo.

8.4.5. Definições avançadas de verificação de vírus

Para além de configurar as definições básicas da verificação de vírus, também pode utilizar as definições avançadas (ver Figura 28):

☑ **Activar tecnologia iChecker** – utiliza a tecnologia que pode aumentar a velocidade de verificação, excluindo determinados objectos da verificação. Um objecto é excluído da verificação, utilizando um algoritmo especial que toma em consideração a data de distribuição das assinaturas de ameaças, a data em que o objecto foi verificado pela última vez e as alterações às definições de verificação.

Por exemplo, você tem um arquivo que o programa analisou e atribuiu a classificação de não infectado. Na próxima vez, o programa vai ignorar este arquivo, a menos que este seja modificado ou as definições alteradas. Se a estrutura do arquivo mudar porque foi adicionado um novo ficheiro, se as definições de verificação foram alteradas ou se as assinaturas de ameaças foram actualizadas, o programa analisará o arquivo novamente.

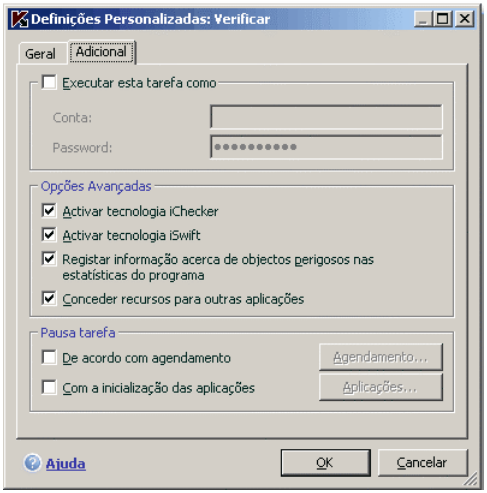


Figura 28. Definições avançadas de verificação

Existem limitações no iChecker™: não funciona com ficheiros extensos e apenas se aplica a ficheiros com uma estrutura que o Kaspersky Anti-Virus para Windows Servers reconheça (por exemplo, .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

Activar tecnologia iSwift – Esta tecnologia é um desenvolvimento da tecnologia iChecker para computadores que usam sistemas de ficheiros NTFS. Existem algumas limitações no iSwift™: está limitado a um local específico para o ficheiro no sistema de ficheiros e aplica-se apenas a objectos em sistemas de ficheiros NTFS.

Registar informação acerca de objectos perigosos nas estatísticas do programa – Guarda informação acerca dos objectos perigosos detectados nas estatísticas gerais do programa e apresenta uma lista das ameaças detectadas durante a verificação no separador **Detectadas** da janela de relatório (ver 11.3.2 na pág. 132). Se esta opção estiver desactivada, a informação acerca de objectos perigosos não será apresentada no relatório e será impossível processar os dados.

Conceder recursos para outras aplicações – pausa aquela tarefa de verificação de vírus se o processador estiver ocupado com outras aplicações.

8.4.6. Estabelecer definições globais para todas as tarefas de verificação

Cada tarefa de verificação é executada de acordo com as suas próprias definições. Por definição, as tarefas criadas, quando você instalou o programa no seu computador, utilizam as definições recomendadas pelos especialistas da Kaspersky Lab.

Você pode configurar as definições globais para todas as tarefas de verificação. Como ponto de partida, você utilizará um conjunto de propriedades utilizadas para procurar vírus num ficheiro individual.

Para atribuir definições globais para todas as tarefas de verificação:

1. Na janela principal no programa, na zona esquerda, seleccione a secção **Verificar** e clique em Definições.
2. Na janela que é aberta, configure as definições da verificação: seleccione o nível de segurança (ver 8.4.1 na pág. 92), configure as definições de nível avançado e seleccione uma acção para objectos (ver 8.4.4 na pág. 97).
3. Para aplicar estas novas definições a todas as tarefas, clique no botão **Aplicar** na secção **Outras definições de tarefa**. Confirme a definições globais que seleccionou na caixa de dialogo que aparece.

CAPÍTULO 9. TESTAR O KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS SERVERS

Depois de instalar e configurar o Kaspersky Anti-Virus, recomendamos que verifique se as definições e o funcionamento do programa estão correctos, usando um vírus de teste e variantes do mesmo.

9.1. O vírus de teste EICAR e as suas variantes

O vírus de teste foi, especialmente, desenvolvido pelo eicar (O Instituto Europeu para Pesquisa de Antivírus de Computador) para testar a funcionalidade de Anti-Vírus.

O vírus de teste NÃO É UM VÍRUS e não contém código de programa que possa danificar o seu computador. Contudo, a maioria dos programas de Anti-Vírus identificá-lo-á como um vírus.

Nunca use vírus reais para testar a funcionalidade de um Anti-Vírus!

Pode transferir um vírus de teste a partir do site oficial do **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

O ficheiro que transferiu do site do **EICAR** contém o corpo de um vírus de teste padrão. O Kaspersky Anti-Virus irá detectá-lo, classificá-lo como um **vírus** e tomar a acção definida para aquele tipo de objecto.

Para testar as reacções do Kaspersky Anti-Virus quando são detectados diferentes tipos de objectos, você pode alterar os conteúdos do vírus de teste padrão, adicionando um dos prefixos apresentados na tabela que se segue.

Prefixo	Estado do vírus de teste	Acção correspondente quando a aplicação processa o objecto
Sem prefixo, vírus de teste padrão	O ficheiro contém um vírus de teste. Não é possível desinfectar o objecto.	A aplicação identificará o objecto como malicioso, não sujeito a tratamento e irá apagá-lo.
`CORR-`	Corrompido.	A aplicação conseguia aceder ao objecto, mas não consegui verificá-lo, uma vez que o objecto está corrompido (por exemplo, a estrutura de ficheiro foi violada ou é um formato inválido).
`SUSP-` `WARN-`	O ficheiro contém um vírus de teste (variante). Não é possível desinfectar o objecto.	Este objecto é uma variante de um vírus conhecido ou um vírus desconhecido. Na altura da detecção, as bases de dados de assinaturas de ameaças não contêm uma descrição do procedimento para tratar este objecto. A aplicação colocará o objecto em Quarentena para ser processado mais tarde com assinaturas de ameaças actualizadas.
`ERRO-`	Erro de processamento.	Ocorreu um erro ao processar o objecto: a aplicação não consegue aceder ao objecto que está a ser verificado, uma vez que a integridade do objecto foi violada (por exemplo, não há fim para um arquivo multi-volume) ou existe ligação para o mesmo (se o objecto está a ser analisado numa unidade de rede).

Prefixo	Estado do vírus de teste	Acção correspondente quando a aplicação processa o objecto
CURE-	O ficheiro contém um vírus de teste. É possível tratá-lo. O objecto é sujeito a desinfecção e o texto do corpo do vírus alterar-se-á para CURE.	O objecto contém um vírus que pode ser tratado. A aplicação analisará o objecto em termos de vírus, após o qual este será completamente tratado.
DELE-	O ficheiro contém um vírus de teste. Não é possível desinfectar o objecto.	Este objecto contém um vírus que não pode ser desinfectado ou é um Trojan. A aplicação apaga estes objectos.

A primeira coluna da tabela contém os prefixos que é necessário adicionar ao início da sequência para um vírus de teste padrão. A segunda coluna descreve o estado e reacção do Kaspersky Anti-Virus aos vários tipos de vírus de teste. A terceira coluna contém informação sobre objectos com o mesmo estado que a aplicação processou.

Os valores presentes nas definições de verificação Anti-Vírus determinam a acção tomada em cada um dos objectos.

9.2. Testar o Anti-Vírus de Ficheiros

Para testar a funcionalidade do Anti-Vírus de Ficheiros;

1. Crie uma pasta num disco, copie para essa pasta o vírus de teste transferido a partir do site oficial da organização (ver 9.1 na pág. 102), e as variantes do vírus de teste que você criou.
2. Permita que todos os eventos sejam registados para que o ficheiro relatório retenha dados sobre objectos corrompidos e objectos não verificados devido a erros. Para o fazer assinale a opção ☑ **Registar eventos não críticos** na janela das definições do relatório (ver 11.3.1 na pág. 131).
3. Execute o vírus de teste ou uma variante do mesmo.

O Anti-Vírus de Ficheiros irá interceptar a sua tentativa para aceder ao ficheiro, irá verificá-lo e apagá-lo.

Quando selecciona diferentes opções de configuração predefinidas para lidar com os objectos detectados, pode testar as reacções do Anti-Vírus de Ficheiros à detecção de vários tipos de objectos.

Pode ver os detalhes sobre o desempenho do Anti-Vírus de Ficheiros no relatório da componente.

9.3. Testar as tarefas de verificação de vírus

Para testar tarefas de verificação de vírus:

1. Crie uma pasta num disco, copie para essa pasta o vírus de teste transferido a partir do site oficial da organização (ver 9.1 na pág. 102) e as variantes do vírus de teste que você criou.
2. Crie uma nova tarefa de verificação de vírus (ver 8.3 na pág. 90) e seleccione a pasta com o conjunto de vírus de teste como os objectos a verificar (ver 9.1 na pág. 102).
3. Permita que todos os eventos sejam registados para que o ficheiro relatório retenha dados sobre objectos corrompidos e objectos não verificados devido a erros. Para o fazer assinale a opção ☑ **Registar eventos não críticos** na janela das definições do relatório.
4. Execute a tarefa de verificação de vírus (ver 8.1 na pág. 88).

Quando executa uma verificação, como são detectados objectos suspeitos ou infectados, são apresentadas notificações no ecrã com informação acerca dos objectos, perguntando ao utilizador qual a próxima acção a tomar:

Figura 29. Objecto perigoso detectado

Desta forma, ao seleccionar diferentes opções de configuração predefinidas para as acções, pode testar as reacções do Anti-Vírus de Ficheiros à detecção de vários tipos de objectos.

Pode ver os detalhes sobre o desempenho de uma tarefa de verificação de vírus no relatório da componente.

CAPÍTULO 10. ACTUALIZAÇÕES DO PROGRAMA

Manter o seu software Anti-Vírus actualizado é um investimento na segurança do seu computador. É importante actualizar regularmente a aplicação de forma a manter a sua informação constantemente protegida, porque novos vírus e novo software malicioso surgem diariamente.

Actualizar a aplicação envolve a transferência e instalação das seguintes componentes no seu computador:

- **Assinaturas de ameaças**

  A aplicação utiliza assinaturas de ameaças para proteger a informação no seu computador. As componentes do software que fornecem a protecção utilizam-nas para procurar e desinfectar ficheiros perigosos no seu computador. As assinaturas são actualizadas todas as horas com novas ameaças e métodos de como as combater. Por isso, recomenda-se que elas sejam actualizadas regularmente.

  As versões anteriores das aplicações da Kaspersky Lab englobavam conjuntos de bases de dados padrão e alargadas. Cada uma delas tratava de proteger o seu computador em relação a tipos diferentes de ficheiros perigosos. No Kaspersky Anti-Virus para Windows Servers não precisamos de nos preocupar com a selecção do conjunto apropriado de assinaturas de ameaças. Agora, os nossos produtos utilizam as assinaturas de ameaças que o protegem tanto dos ficheiros maliciosos e potencialmente perigosos variados como dos ataques de hackers.

- **Módulos do programa**

  Além das assinaturas, pode actualizar os módulos internos do Kaspersky Anti-Virus para Windows Servers. Surgem, regularmente, novas actualizações da aplicação.

A origem principal de actualização do Kaspersky Anti-Virus para Windows Servers são os servidores de actualização da Kaspersky Lab.

Para transferir as actualizações disponíveis a partir dos servidores de actualização, o seu computador tem de estar ligado à Internet.

Se não tiver acesso aos servidores de actualização da Kaspersky Lab (por exemplo, o seu computador não está ligado à Internet), pode ligar para a sede da Kaspersky Lab +7 (495) 797-87-00, +7 (495) 645-79-39 ou +7 (495) 956-70-00 para pedir informação de contacto dos parceiros da Kaspersky Lab que lhe possam fornecer actualizações comprimidas em disquetes ou CDs.

As actualizações podem ser transferidas através de um dos seguintes modos:

- *Automaticamente.* O Kaspersky Anti-Virus verifica, em intervalos especificados, se existem pacotes de actualização na origem de actualização. As verificações podem ser definidas para serem mais frequentes durante surtos de vírus e menos frequentes quando esses surtos terminam. Quando o Anti-Vírus detecta novas actualizações, transfere-as e instala-as no computador. Esta é a opção predefinida.
- *De acordo com agendamento*. A actualização está estipulada para começar numa altura específica.
- *Manualmente.* Com esta opção, você inicializa manualmente o Actualizador.

Durante a actualização, a aplicação compara as assinaturas de ameaças e os módulos da aplicação existentes no servidor com as versões disponíveis no servidor de actualização. Se o servidor tiver a última versão das assinaturas e módulos da aplicação, aparecerá uma notificação sobre isso na janela da aplicação. Se as assinaturas e módulos existentes no servidor e no servidor de actualizações diferirem, a aplicação só transferirá as partes que faltam das actualizações. O Actualizador não transfere assinaturas e módulos que você já tenha, o que aumenta, significativamente, a velocidade de transferência e poupa tráfego de Internet.

Antes de actualizar as assinaturas de ameaças, o Kaspersky Anti-Virus para Windows Servers cria cópias de segurança das mesmas, que podem ser utilizadas se for necessário reverter para a última versão das assinaturas (ver 10.2 na pág. 109). Se, por exemplo, o processo de actualização corrompe as assinaturas de ameaças e deixa-as inutilizáveis, você pode facilmente reverter para a versão anterior e tentar actualizar as assinaturas mais tarde.

Você pode distribuir as actualizações para uma origem local ao mesmo tempo que actualiza a aplicação (ver 10.4.4 na pág. 118). Esta função permite-lhe actualizar bases de dados e módulos usados pelas aplicações da versão 6.0 em computadores de rede para poupar na largura de banda.

10.1. Iniciar o Actualizador

Pode começar o processo de actualização em qualquer altura. Este funcionará a partir da origem de actualização que você seleccionar (ver 10.4.1 na pág. 111).

Pode iniciar o Actualizador a partir:

- do menu de contexto (ver 4.2 na pág. 39)
- da janela principal do programa (ver 4.3 na pág. 40)

Para iniciar o Actualizador a partir do menu de contexto:

1. Clique com o botão direito do rato no ícone da aplicação na bandeja do sistema para abrir o menu de contexto.
2. Seleccione **Actualização**.

Para iniciar o Actualizador a partir da janela principal do programa:

1. Seleccione **Actualização** na secção **Serviço**.
2. Clique em **Actualizar agora!** no painel direito da janela principal ou utilize o botão ▶ da barra de estado.

O progresso da actualização será exibido numa janela especial. Pode esconder a janela de progresso de actualização. Para o fazer, clique em **Fechar**. A actualização continuará com a janela escondida.

Note que as actualizações são distribuídas na origem local durante o processo de actualização, desde que este serviço esteja activado (ver 10.4.4 na pág. 118).

10.2. Reverter para a actualização anterior

Sempre que iniciar o Actualizador, o Kaspersky Anti-Virus para Windows Servers primeiro cria uma cópia de segurança das actuais assinaturas de ameaças e só depois inicia a transferência das actualizações. Desta forma, você pode voltar a utilizar a versão anterior das assinaturas se a actualização falhar.

Para voltar à versão anterior das assinaturas de ameaças:

1. Seleccione a componente **Actualização** na secção **Serviço** na janela principal do programa.
2. Clique no botão **Reversão** no painel direito da janela principal do programa.

10.3. Criar tarefas de actualização

O Kaspersky Anti-Virus tem integrada uma tarefa de actualização para actualizar módulos do programa e assinaturas de ameaças. Também pode criar as suas próprias tarefas de actualização com várias definições e agendamentos.

Por exemplo, você instalou o Kaspersky Anti-Virus num portátil que usa em casa e no trabalho. Em casa, você actualiza o programa a partir dos servidores de

actualização da Kaspersky Lab e no trabalho actualiza a partir de uma pasta local que guarda as actualizações de que necessita. Utilize duas tarefas diferentes para evitar ter que mudar as definições de actualização sempre que muda de local.

Para criar uma tarefa de actualização avançada:

1. Seleccione **Actualização** na secção **Serviço** da janela principal do programa, abra o menu de contexto, clicando com o botão direito, e seleccione **Guardar como**.
2. Insira o nome para a tarefa na janela que se abre e clique em **OK**. Aparecerá uma tarefa com esse nome na secção **Serviço** da janela principal do programa.

Aviso!

Existe um limite para o número de tarefas de actualização que o utilizador pode criar no Kaspersky Anti-Virus. O número máximo é duas tarefas.

A nova tarefa herda todas as propriedades da tarefa na qual se baseou para criar a nova tarefa, excepto no que diz respeito às definições de agendamento. Para esta nova tarefa, é desactivada a definição de verificação automática que existe por defeito. Terá de continuar a configuração, especificando a origem de actualização (ver 10.4.1 na pág. 111), as definições de ligação de rede (ver 10.4.3 na pág. 116) e, se necessário, activando as tarefas com privilégios (ver 6.4 na pág. 67) e configurando o horário agendado (ver 6.5 na pág. 68).

Para mudar o nome de uma tarefa:

Seleccione a tarefa na secção **Serviço** da janela principal do programa, abra o meu de contexto, clicando com o botão direito do rato, e seleccione **Mudar nome**.

Insira o novo nome para a tarefa na janela que se abre e clique em **OK**. O nome da tarefa será então alterado na secção **Serviço**.

Para apagar uma tarefa:

Seleccione a tarefa na secção **Serviço** da janela principal do programa, abra o menu de contexto, clicando com o botão direito do rato, e seleccione **Apagar**.

Na janela de confirmação, confirme que pretende apagar a tarefa. A tarefa será então apagada da lista de tarefas na secção **Serviço**.

Aviso!

Apenas pode alterar o nome e apagar tarefas personalizadas.

10.4. Configurar as definições de actualização

O Actualizador funciona com definições que regulam o seguinte:

- A origem a partir da qual são transferidas e instaladas as actualizações (ver 10.4.1 na pág. 111);
- O modo de execução da actualização da aplicação e as componentes específicas actualizadas (ver 10.4.2 na pág. 114);
- Com que frequência será executada a actualização, se agendada (ver 6.5 na pág. 68);
- Com que conta de utilizador será executada a actualização (ver 6.4 na pág. 67);
- O requisito para copiar actualizações transferidas para um directório local (ver 10.4.4 na pág. 118);
- Quais as acções que deve efectuar depois de concluída a actualização (ver 10.4.5 na pág. 119).

As secções que se seguem irão examinar, em detalhe, estes aspectos.

10.4.1. Seleccionar uma origem de actualização

A *origem de actualização* é um recurso que contém as actualizações para as assinaturas de ameaças e para os módulos da aplicação do Kaspersky Anti-Virus.

Pode usar as seguintes origens de actualização:

- *Servidor de Administração* – uma área centralizada para armazenamento de actualizações, localizada no Servidor de Administração do Kaspersky Administration Kit (para mais detalhes, veja o Manual do Utilizador do Kaspersky Administration Kit 6.0).
- *Servidores de actualização da Kaspersky Lab* – sites especiais que contêm as actualizações disponíveis para as assinaturas de ameaças e módulos da aplicação de todos os produtos da Kaspersky Lab.
- *Servidor de HTTP ou FTP ou pasta local ou de rede* – servidor ou pasta local que contém as últimas actualizações.

Se não tiver acesso aos servidores de actualização da Kaspersky Lab (por exemplo, não possui ligação à Internet), pode ligar para a sede da Kaspersky Lab +7 (495) 797-87-00, 7 (495) 645-79-39 ou +7 (495) 956-70-00 para pedir informação de contacto dos parceiros da Kaspersky Lab que lhe possam fornecer actualizações comprimidas em disquetes ou CDs.

Aviso!

Ao solicitar actualizações em meios removíveis, por favor especifique se também deseja as actualizações para os módulos internos da aplicação.

Pode copiar as actualizações a partir de um disco e transferi-las para um site FTP ou HTTP ou guardá-las numa pasta local ou da rede.

Seleccione a origem da actualização no Separador **Origem da actualização** (ver Figura 30).

O opção predefinida transfere actualizações dos servidores de actualização dos servidores da Kaspersky Lab. A lista de endereços que este item representa não pode ser editada. Ao actualizar, o Kaspersky Anti-Virus para Windows Servers chama esta lista, selecciona o endereço do primeiro servidor e tenta transferir os ficheiros a partir desse servidor. Se as actualizações não poderem ser transferidas a partir do primeiro servidor, a aplicação tenta ligar-se a cada um dos servidores seguintes até ser bem sucedida.

Para transferir actualizações de outro site FTP ou HTTP:

1. Clique em **Adicionar.**
2. Na caixa de diálogo **Seleccionar origem de actualização**, seleccione o site alvo FTP ou HTTP ou especifique, no campo **Origem,** o endereço IP, nome do caractere ou endereço URL deste site. Ao seleccionar um site ftp como uma origem de actualização, as definições de autenticação devem ser inseridas no URL do servidor com o seguinte formato ftp://<user_name>:<password>@<host>:<port>.

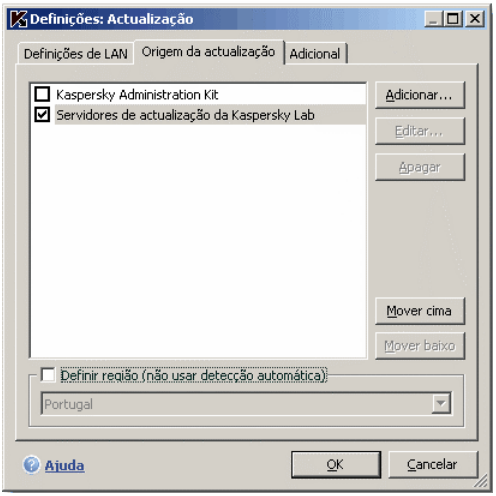


Figura 30. Seleccionar uma origem da actualização

Aviso!

Se seleccionou um recurso localizado fora da LAN (Rede de Área Local) como uma origem de actualização, então necessita de uma ligação à Internet para efectuar a actualização.

Para actualizar a partir de uma pasta local:

1. Clique **Adicionar.**
2. Na caixa de diálogo **Seleccionar Origem de Actualização**, seleccione uma pasta ou especifique o atalho completo para esta pasta no campo **Origem**.

O Kaspersky Anti-Virus para Windows Servers adiciona uma nova origem de actualização ao topo da lista e assinala, automaticamente, esta origem como estando activada.

Se vários recursos são seleccionados como origens de actualização, a aplicação tenta ligar-se a eles um após o outro, começando no topo da lista e restabelece as actualizações a partir da primeira origem disponível. Pode alterar a ordem das origens na lista, utilizando os botões **Mover cima** e **Mover baixo**.

Para editar esta lista, utilize os botões **Adicionar**, **Editar** e **Remover**. Não pode editar ou apagar os servidores de actualização da Kaspersky Lab ou do Kaspersky Administration Kit.

Se utilizar os servidores de actualização da Kaspersky Lab como origem de actualização, pode seleccionar a localização optimizada do servidor para

transferir actualizações. A Kaspersky Lab possui servidores em vários países. Ao escolher o servidor de actualização da Kaspersky Lab mais próximo de si, poupa tempo e efectuará mais rapidamente as transferências de actualizações.

Para escolher o servidor mais próximo, seleccione **Definir região (não usar detecção automática)** e seleccione o país mais próximo da sua actual localização a partir da lista pendente. Se assinalar esta caixa, as actualizações serão executadas tendo em consideração a região seleccionada na lista. Por defeito, esta caixa está desmarcada e é usada a informação acerca da actual região do registo do sistema operativo.

10.4.2. Seleccionar o método de actualização e o que actualizar

Ao configurar as definições de actualização, é importante definir o que actualizar e qual o método de actualização a utilizar.

Os objectos de actualização (ver Figura 31) são as componentes a serem actualizadas:

- assinaturas de ameaças;
- módulos do programa.

As assinaturas de ameaças são sempre actualizadas, enquanto os módulos da aplicação só são actualizados se as definições estiverem configuradas para tal.

Figura 31. Seleccionar objectos de actualização

Se deseja transferir e instalar actualizações para os módulos do programa:

Seleccione **Actualizar módulos da aplicação** na janela **Actualização**.

Se existir uma actualização dos módulos da aplicação na origem de actualização, a aplicação transferirá as actualizações necessárias e aplicá-las-á depois do sistema ser reiniciado. As actualizações dos módulos transferidas só serão instaladas depois do computador ser reiniciado.

Se a próxima actualização do programa acontecer antes do computador ser reiniciado e antes das actualizações dos módulos do programa

anteriormente transferidas serem instaladas, só serão actualizadas as assinaturas de ameaças.

O Método de Actualização (ver Figura 32) define como é que o Actualizador é iniciado. Pode escolher um destes métodos na secção **Modo de Execução**:

- **Automaticamente** – O Kaspersky Anti-Virus verifica, em intervalos especificados, se existem pacotes de actualização na origem de actualização (ver 10.4.1 na pág. 111). Quando o Anti-Vírus detecta novas actualizações, transfere-as e instala-as no computador.

  Se um recurso de rede for especificado como origem de actualização, o Kaspersky Anti-Virus tenta iniciar o Actualizador depois de um determinado período de tempo, conforme o especificado no anterior pacote de actualização.

  Se for seleccionada uma pasta local como origem de actualização, a aplicação tenta transferir as actualizações a partir da pasta local com a frequência especificada no pacote de actualização transferido durante a última actualização. Esta opção permite à Kaspersky Lab regular a frequência de actualização do programa no caso de surtos de vírus aparecer e noutras situações potencialmente perigosas. A sua aplicação receberá as últimas actualizações para as assinaturas de ameaças, ataques de rede e módulos do software de forma atempada, prevenindo desta forma a entrada de software malicioso no servidor.

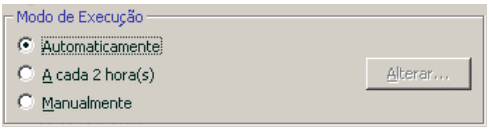


Figura 32. Seleccionar o modo de execução das actualizações

- **De acordo com agendamento**. A actualização está agendada para começar num momento especificado. Por defeito, as actualizações agendadas ocorrerão a cada 2 horas. Para editar o agendamento predefinido, clique no botão **Alterar...** junto ao título do modo e faça as alterações necessárias na janela que se abre (para mais detalhes, ver 6.5 na pág. 68). Este modo é utilizado por defeito.
- **Manualmente**. Com esta opção, você inicializa manualmente o Actualizador. O Kaspersky Anti-Virus para Windows Servers notifica-o quando precisa de o actualizar:

  - Primeiro, em cima do ícone de bandeja do sistema, aparece uma mensagem de pop-up a informá-lo de que a actualização é necessária (se os avisos estiverem activados; ver 11.8.1 na pág. 144);
  - O segundo indicador na janela principal do programa informa-o de que o seu computador está desactualizado (ver 5.1.1 na pág. 45);

- Surge uma recomendação para actualização da aplicação na secção de mensagens na janela principal do programa (ver 4.3 na pág. 40).

10.4.3. Configurar as definições de ligação de rede

Se configurar o programa para ir buscar actualizações aos servidores de actualização da Kaspersky Lab ou a outros sites FTP ou HTTP, recomendamos que verifique primeiro as suas definições de ligação de rede.

Todas as definições estão agrupadas num separador especial – **Definições de LAN** (ver Figura 33).

Seleccione **Utilizar modo FTP passivo se possível** se transferir as actualizações a partir de um servidor FTP em modo passivo (por exemplo, através de uma firewall). Se estiver a trabalhar em modo FTP activo, desmarque esta caixa de selecção.

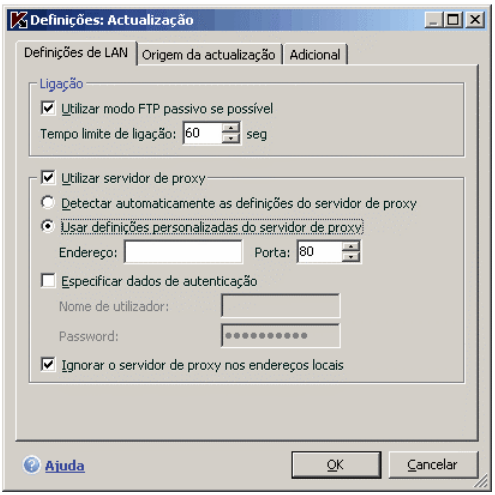


Figura 33. Configurar definições de actualização da rede

No campo **Tempo limite de ligação … (seg)**, defina o tempo atribuído para a ligação ao servidor de actualização. Se a ligação falhar, depois deste tempo ter decorrido o programa tentará ligar-se ao próximo servidor de actualização. Isto continua até que seja estabelecida uma ligação com sucesso ou até tentar todos os servidores de actualização disponíveis.

Seleccione **Utilizar servidor de proxy** se estiver a utilizar um servidor de proxy para aceder à Internet e, se necessário, seleccione as seguintes definições:

- Seleccione as definições do servidor de proxy que serão utilizadas durante a actualização:

  Detectar automaticamente as definições do servidor de proxy. Se seleccionar esta opção, as definições de proxy são detectadas automaticamente através do protocolo WPAD (Web Proxy Auto-Discovery Protocol). Se este protocolo não conseguir detectar o endereço, o Kaspersky Anti-Virus usará as definições do servidor de proxy especificadas no Microsoft Internet Explorer.

  Usar definições personalizadas do servidor de proxy– utilize um proxy diferente do especificado nas definições de ligação do navegador. No campo **Endereço**, introduza ou o endereço IP ou o nome simbólico do servidor de proxy e no campo **Porta** especifique o número da porta de proxy.

- Especifique se é necessária autenticação no servidor de proxy. *Autenticação* é o processo de verificação dos dados de registo do utilizador para fins de controlo de acesso.

  Se for necessária autenticação para ligar ao servidor de proxy, assinale a opção **Especificar dados de autenticação** e especifique o nome de utilizador e password nos campos que surgem em baixo. Nesse caso, primeiro tenta-se a autenticação por NTLM e depois a autenticação por BASIC.

  Se esta caixa não estiver seleccionada ou se os dados não forem inseridos, a autenticação por NTLM será tentada, utilizando a conta de utilizador usada para iniciar a actualização (ver 6.4 na pág. 67).

  Se o servidor de proxy requer **Nome de utilizador** e você não tiver introduzido o nome de utilizador e **Password** ou, se por alguma razão, os dados especificados não tiverem sido aceites pelo servidor de proxy, surgirá uma janela quando a actualização começar, pedido o nome de utilizador e password para autenticação. Se a autenticação for bem-sucedida, o nome de utilizador e password serão utilizados nas próximas actualizações. Caso contrário, as definições serão novamente solicitadas.

Para evitar utilizar uma proxy quando a origem de actualização é uma pasta local, seleccione a opção **Ignorar o servidor de proxy nos endereços locais**.

10.4.4. Distribuição de actualizações

A função de cópia de actualizações permite optimizar a carga na rede da sua empresa. As actualizações são copiadas em duas etapas:

1. Um dos computadores da rede recolhe um pacote de actualização da aplicação e das assinaturas de ameaças a partir dos servidores da Kaspersky Lab ou a partir de outro recurso da Internet que aloja um conjunto de actualizações correntes. As actualizações recolhidas são colocadas numa pasta de acesso público.
2. Os outros computadores da rede acedem à pasta de acesso público para recolher as actualizações da aplicação.

Para activar a distribuição de actualizações, seleccione a caixa **Pasta de distribuição de actualizações** no separador **Adicional** (ver Figura 34) e no campo por baixo especifique a pasta partilhada onde serão colocadas as actualizações recolhidas. Pode introduzir o caminho manualmente ou seleccioná-lo na janela que se abre quando clica em **Procurar.** Se seleccionar a caixa, as actualizações serão, automaticamente, copiadas para esta pasta quando forem recolhidas.

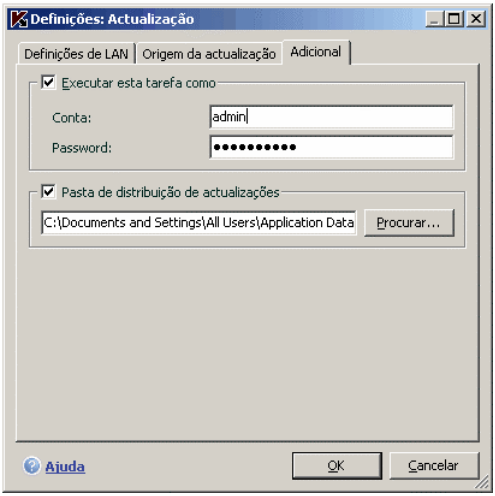


Figura 34. Definições da ferramenta de cópia de actualizações

Também pode especificar o método de distribuição das actualizações:

- *completa*, que copia as assinaturas de ameaças e actualizações das componentes para todas as aplicações 6.0 da Kaspersky Lab 6.0. Para

seleccionar as actualizações completas, seleccione a caixa ☑ **Copiar actualizações para todas as componentes da aplicação**.

- *personalizada*, que apenas copia as assinaturas de ameaças e actualizações para as componentes do Kaspersky Anti-Virus 6.0 que estão instaladas. Se deseja seleccionar este método de actualização, você tem que desmarcar a caixa ☑ **Copiar actualizações para todas as componentes da aplicação**.

Se quiser que outros computadores da rede actualizem a partir da pasta que contém as actualizações copiadas da Internet, tem que seguir os seguintes passos:

1. Conceder acesso público a esta pasta.
2. Especificar a pasta partilhada como a origem da actualização nos computadores da rede, nas definições do Actualizador.

10.4.5. Acções depois de actualizar o programa

Cada actualização de assinaturas de ameaças contém registos novos que protegem o seu computador das últimas ameaças.

A Kaspersky Lab recomenda a verificação dos ficheiros em quarentena e dos objectos de inicialização sempre que a base de dados for actualizada.

Porque é que estes ficheiros devem ser analisados?

A quarentena contém ficheiros que foram marcados pelo programa como suspeitos ou possivelmente infectados (ver 11.1 na pág. 122). Utilizando a última versão das assinaturas de ameaças, o Kaspersky Anti-Virus para Windows Servers poderá identificar a ameaça e eliminá-la.

Por definição, a aplicação analisa os ficheiros em quarentena depois de cada actualização das assinaturas de ameaças. Também recomendamos que examine, periodicamente, os ficheiros em quarentena porque o seu estado pode alterar-se após várias verificações. Alguns ficheiros podem então ser restaurados às localizações prévias e poderá continuar a trabalhar com eles.

Para desactivar a verificação dos ficheiros em quarentena, desmarque a opção ☑ **Verificar novamente a Quarentena** na secção **Acção após Actualização**.

Os objectos de inicialização são críticos para a segurança do seu computador. Se um deles estiver infectado com uma aplicação maliciosa, isto pode levar a uma falha na inicialização do sistema operativo. O Kaspersky Anti-Virus para Windows Servers possui uma tarefa de verificação incorporada para os objectos de inicialização (ver Capítulo 8 na pág. 87). Recomendamos que estabeleça um

agendamento para esta tarefa de forma a que seja automaticamente iniciada após cada actualização das assinaturas de ameaças (ver 6.5 na pág. 68).

CAPÍTULO 11. OPÇÕES AVANÇADAS

O Kaspersky Anti-Virus para Windows Servers possui outras características que aumentam a sua funcionalidade.

O programa coloca alguns ficheiros em áreas de armazenamento especiais. Isto assegura a protecção máxima dos dados com perdas mínimas.

- A cópia de segurança contém cópias de ficheiros que o Kaspersky Anti-Virus para Windows Servers alterou ou apagou (ver 11.2 na pág. 125). Se algum ficheiro continha informação que era importante para si e que não pôde ser totalmente recuperada durante o processamento do Anti-Vírus, pode sempre restaurar o ficheiro a partir desta cópia de segurança.
- A quarentena contém ficheiros, potencialmente, infectados que não puderam ser processados utilizando as actuais assinaturas de ameaças (ver 11.1 na pág. 122).

Recomenda-se que examine, periodicamente, a lista de ficheiros. Alguns deles podem já estar desactualizados e alguns podem ter sido restaurados.

Algumas das características foram concebidas para o ajudar enquanto utiliza o programa. Por exemplo:

- O Suporte Técnico fornece assistência polivalente com o Kaspersky Anti-Virus para Windows Servers (ver 11.6 na pág. 139). A Kaspersky Lab fornece-lhe todos os meios de apoio possíveis: apoio on-line, um fórum de perguntas e respostas para os utilizadores do programa, etc.
- A funcionalidade Notificações disponibiliza ao utilizador notificações sobre momentos-chave no Kaspersky Anti-Virus para Windows Servers (ver 11.8.1 na pág. 144). Podem ser eventos com natureza informativa ou erros que devem ser imediatamente eliminados e sobre os quais é necessário ter conhecimento.
- A Autodefesa protege os ficheiros do próprio programa de serem modificados ou danificados por hackers, bloqueia a administração remota da utilização das funcionalidades do programa e restringe os direitos do administrador do servidor no seu computador na execução de certas acções no Kaspersky Anti-Virus para Windows Servers (ver 11.8.2 na pág. 148). Por exemplo, alterar o nível de protecção pode influenciar, significativamente, a segurança da informação no seu computador.

- O Gestor da Chave de Licença pode obter informação detalhada sobre a licença utilizada, activar a sua cópia do programa e gerir ficheiros de chaves de licença (ver 11.5 na pág. 137).

O programa também fornece uma secção de Ajuda (ver 11.4 na pág. 136) e relatórios detalhados (ver 11.3 na pág. 128) sobre o funcionamento do Anti-Vírus de Ficheiros e tarefas de verificação de vírus e de actualização.

Você também pode alterar o aspecto do Kaspersky Anti-Virus para Windows Servers e pode personalizar a interface do programa (ver 11.7 na pág. 141).

As secções que se seguem irão discutir, em detalhe, estas funções.

11.1. Quarentena para objectos potencialmente infectados

A **Quarentena** é uma área de armazenamento especial que contém ficheiros, potencialmente, infectados com vírus.

Os **ficheiros, potencialmente, infectados** são ficheiros que se suspeita estarem infectados com vírus ou modificações de vírus.

Porquê *potencialmente infectados*? Nem sempre é possível determinar se um ficheiro está infectado. Isto pode acontecer por várias razões:

- O código do objecto analisado é parecido com uma ameaça conhecida mas está parcialmente modificado.

  As assinaturas de ameaças contêm ameaças que já foram estudadas pela Kaspersky Lab. Se um programa malicioso é modificado e estas alterações ainda não foram introduzidas nas assinaturas, o Kaspersky Anti-Virus para Windows Servers classifica o objecto infectado com o programa malicioso alterado como um objecto, potencialmente, infectado e indicará a ameaça com a qual esta infecção se assemelha.

- O código do objecto detectado faz lembrar a estrutura de uma sequência de vírus de um programa malicioso. No entanto, não existe nada similar nas assinaturas de ameaça.

  É possível que seja um novo tipo de ameaça, por isso o Kaspersky Anti-Virus para Windows Servers classifica o objecto como um objecto, potencialmente, infectado.

O analisador do código *heurístico* detecta vírus potenciais. O mecanismo é bastante eficaz e muito raramente produz falsos diagnósticos positivos.

Um ficheiro potencialmente infectado pode ser detectado e colocado em quarentena pelo Anti-Vírus Ficheiros ou durante uma verificação de vírus.

Pode colocar um ficheiro em quarentena clicando em **Quarentena** na notificação que aparece quando é detectado um ficheiro potencialmente infectado.

Quando coloca um ficheiro em Quarentena, este é movido e não copiado. O ficheiro é apagado do disco ou do e-mail e é guardado na pasta Quarentena. Os ficheiros em Quarentena são guardados num formato especial e não são perigosos.

11.1.1. Acções com objectos em quarentena

O número total de ficheiros em **Quarentena** é exibido na secção **Ficheiros de Dados** do **Serviço**. Na parte direita do ecrã, a secção *Quarentena* mostra:

- o número de ficheiros potencialmente infectados detectados durante o funcionamento do Kaspersky Anti-Virus para Windows Servers;
- o tamanho actual da Quarentena.

Aqui pode apagar todos os ficheiros em quarentena com o botão **Limpar**. Note que ao fazer isso os ficheiros de da cópia de segurança e ficheiros de relatórios também serão apagados.

Para aceder aos objectos em Quarentena:

Clique com o botão esquerdo do rato na secção **Quarentena**.

Pode efectuar as seguintes acções no Separador **Quarentena** (ver Figura 35):

- Mover para a Quarentena um ficheiro que você suspeita estar infectado, mas que o programa não detectou. Para o fazer, clique em **Adicionar** e seleccione o ficheiro de que necessita na janela de selecção. Será adicionado à lista com o estado *adicionado pelo utilizador*.
- Analisar e desinfectar todos os objectos potencialmente infectados na Quarentena utilizando as assinaturas de ameaças actuais. Para o fazer, clique em **Verificar todos**.

  Depois de analisar e desinfectar qualquer objecto em quarentena, o seu estado poderá alterar-se para *infectado, potencialmente infectado, falso diagnóstico positivo, OK*, etc.

  O estado *infectado* significa que o objecto foi identificado como infectado mas não pôde ser tratado. Recomendamos que apague esses objectos.

  Todos os objectos marcados como *falsos diagnósticos positivos* podem ser restaurados, já que o seu estado anterior de *potencialmente infectados* não foi confirmado pelo programa ao ser novamente analisado.

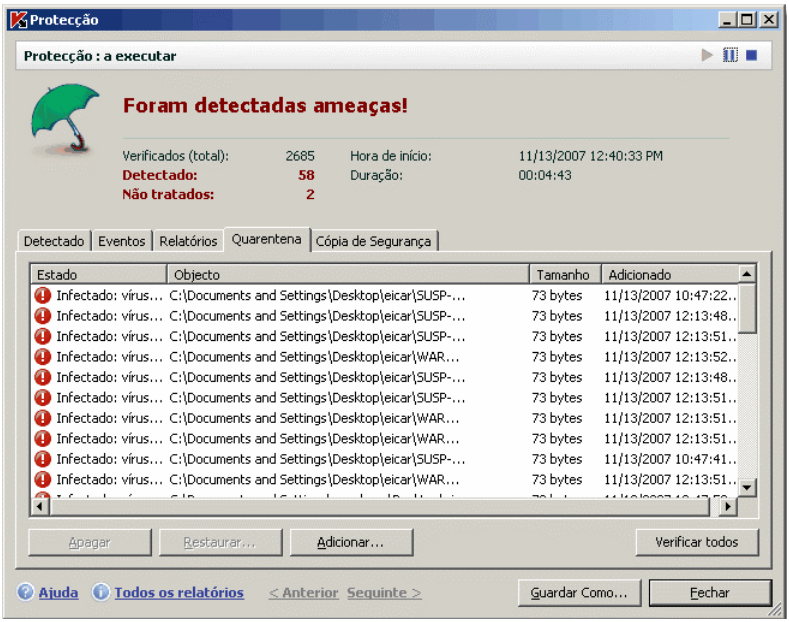


Figura 35. Lista de objectos em quarentena

- Restaurar os ficheiros para uma pasta seleccionada ou para a sua pasta original anterior à Quarentena (opção predefinida). Para restaurar um ficheiro, seleccione-o de uma lista e clique em **Restaurar**. Quando restaurar ficheiros a partir de arquivos, bases de dados de e-mails e ficheiros com formato de e-mail colocados na Quarentena, também deverá seleccionar o directório para o qual os restaura.

> Dica:
>
> Recomendamos que só restaure os objectos com o estado *falso diagnóstico positivo, OK, desinfectado*, já que ao restaurar outros ficheiros pode levar à infecção do seu computador.

- Apagar qualquer objecto ou grupo de objectos seleccionados em quarentena. Apenas apague ficheiros que não possam ser desinfectados. Para apagar ficheiros, seleccione-os na lista e clique em **Apagar**.

11.1.2. Configurar a Quarentena

Pode definir as definições para o esquema de funcionamento da Quarentena, especificamente:

- Configurar verificações automáticas para os objectos em Quarentena depois de cada actualização das assinaturas de ameaças (para mais detalhes, ver 10.4.4 na pág. 118).

  > Aviso!
  >
  > Se estiver a utilizar a Quarentena, o programa não poderá verificar objectos em quarentena, imediatamente, a seguir à actualização das assinaturas de ameaças.

- Estabelecer o tempo máximo de armazenamento na Quarentena.

  O tempo de armazenamento predefinido é de 30 dias, ao fim do qual os ficheiros são apagados. Você pode alterar o tempo de armazenamento da Quarentena ou desactivar esta restrição.

Para o fazer:

1. Abra a janela de definições do Kaspersky Anti-Virus para Windows Servers, clicando em Definições na janela principal do programa.
2. Seleccione **Ficheiros de Dados** na árvore de definições.
3. Na secção **Quarentena e Cópia de Segurança** (ver Figura 36), introduza o período de tempo após o qual os ficheiros em Quarentena serão automaticamente apagados. Em alternativa, desmarque a caixa para desactivar a eliminação automática.

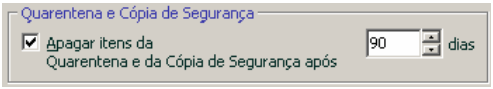


Figura 36. Configurar o período de armazenamento em Quarentena

11.2. Cópias de segurança de objectos perigosos

Algumas vezes, quando os ficheiros são desinfectados, a sua integridade perde-se. Se um ficheiro desinfectado contém informação importante e se depois da desinfecção essa informação é parcial ou completamente corrompida, pode tentar restaurá-lo a partir de uma cópia de segurança.

Uma cópia de segurança é uma cópia do ficheiro perigoso original que é criada quando o ficheiro é primeiro desinfectado ou apagado. É guardado na **Cópia de Segurança**.

A **Cópia de Segurança** é uma área de armazenamento especial que contém as cópias de segurança de ficheiros perigosos que necessitam ser desinfectados ou apagados. A Cópia de Segurança permite-lhe restaurar um ficheiro original em qualquer altura. Os ficheiros são guardados na Cópia de Segurança com um formato especial e não são perigosos.

11.2.1. Acções com cópias de segurança

O número total de cópias de segurança de ficheiros na **Cópia de Segurança** é exibido nos **Ficheiros de Dados** na secção Serviço. Na parte direita do ecrã, a secção *Cópia de Segurança* exibe:

- o número de cópias de segurança de ficheiros criadas pelo Kaspersky Anti-Virus para Windows Servers
- o tamanho actual da Cópia de Segurança.

Aqui pode apagar todas as cópias armazenadas em Cópias de Segurança com o botão **Limpar**. Note que ao fazer isto, os ficheiros em Quarentena e os ficheiros de relatórios também serão apagados.

Para aceder à cópia de ficheiros perigosos:

Clique com o botão esquerdo do rato na secção **Cópia de Segurança**.

Uma lista das cópias de segurança é exibida no Separador **Cópia de Segurança** (ver Figura 37). A seguinte informação é exibida para cada cópia: nome do ficheiro com o atalho para a localização original, estado do ficheiro atribuído pela verificação e o seu tamanho.

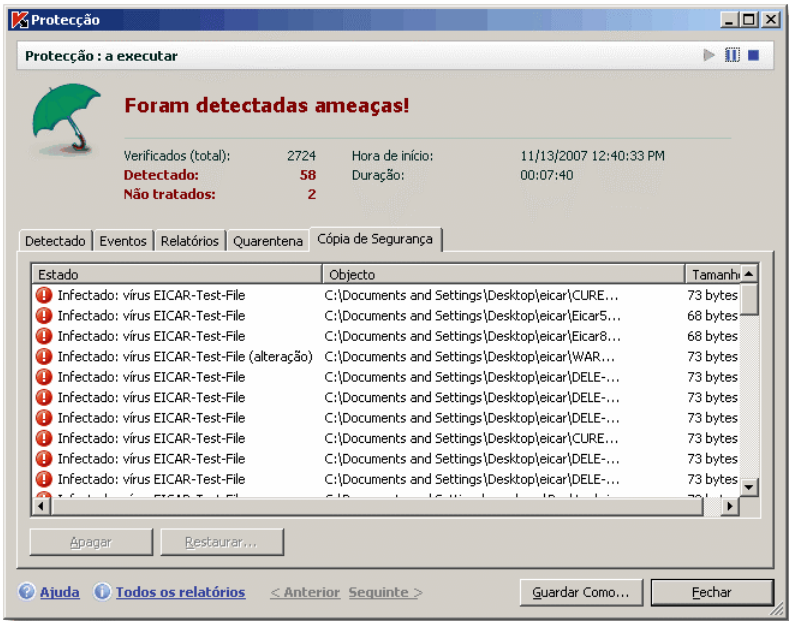


Figura 37. Cópias de segurança de objectos apagados ou desinfectados

Pode restaurar as cópias seleccionadas utilizando o botão **Restaurar**. O ficheiro é restaurado a partir de uma Cópia de Segurança, mantendo o mesmo nome que possuía antes da desinfecção.

Se já há um ficheiro na localização original com esse nome (é possível, se foi feita uma cópia do ficheiro a ser restaurado antes da desinfecção), surgirá o aviso correspondente. Pode alterar a localização do ficheiro restaurado ou dar-lhe um novo nome.

Recomendamos a verificação do ficheiro, imediatamente, a seguir a restaurá-lo. É possível que com as assinaturas actualizadas, você possa desinfectá-lo sem perder a integridade do ficheiro.

Desaconselhamos o restaurar de cópias de segurança de ficheiros, a menos que seja absolutamente necessário. Isto pode levar a uma infecção no seu computador.

Recomendamos que examine, periodicamente, a Cópia de Segurança e a esvazie utilizando o botão **Apagar**. Também pode configurar o programa para que ele apague, automaticamente, as cópias de Segurança mais antigas (ver 11.2.2 na pág. 128).

11.2.2. Configurar as definições de Cópia de Segurança

Pode definir o tempo máximo de armazenamento na Cópia de Segurança.

O tempo de armazenamento predefinido da Cópia de Segurança é de 90 dias, ao fim do qual os ficheiros são apagados. Você pode alterar este tempo de armazenamento ou desactivar esta restrição. Para o fazer:

1. Abra a janela de definições do Kaspersky Anti-Virus para Windows Servers clicando em Definições na janela principal do programa.
2. Seleccione **Ficheiros de Dados** na árvore de definições.
3. Na secção **Quarentena e Cópia de Segurança** (ver Figura 36) estabeleça a duração para o armazenamento das cópias de segurança, na parte direita do ecrã. Em alternativa, desmarque a caixa para desactivar a eliminação automática.

11.3. Relatórios

O desempenho do Anti-Vírus de Ficheiros e de cada tarefa de verificação de vírus e de actualização é guardado num relatório.

O número total de relatórios criados pelo programa e o seu tamanho total é exibido nos **Ficheiros de Dados** na secção **Serviço** na janela principal do Programa. Esta informação é exibida na caixa *Relatórios*.

Para visualizar os relatórios:

Clique com o botão esquerdo do rato na caixa *Relatórios* para abrir a janela Protecção, que resume a protecção fornecida pela aplicação. Uma janela abrir-se-á para o separador **Relatórios** (ver Figura 38).

O separador Relatórios lista os últimos relatórios sobre o Anti-Vírus de Ficheiros e sobre todas as tarefas de verificação de vírus e actualizações efectuadas durante a actual sessão do Kaspersky Anti-Virus para Windows Servers. O estado é listado junto ao Anti-Vírus de Ficheiros ou tarefa, por exemplo, *parado ou concluído*. Se deseja visualizar todo o historial da criação de relatórios para a actual sessão do programa, seleccione ☑ **Mostrar histórico de relatórios**.

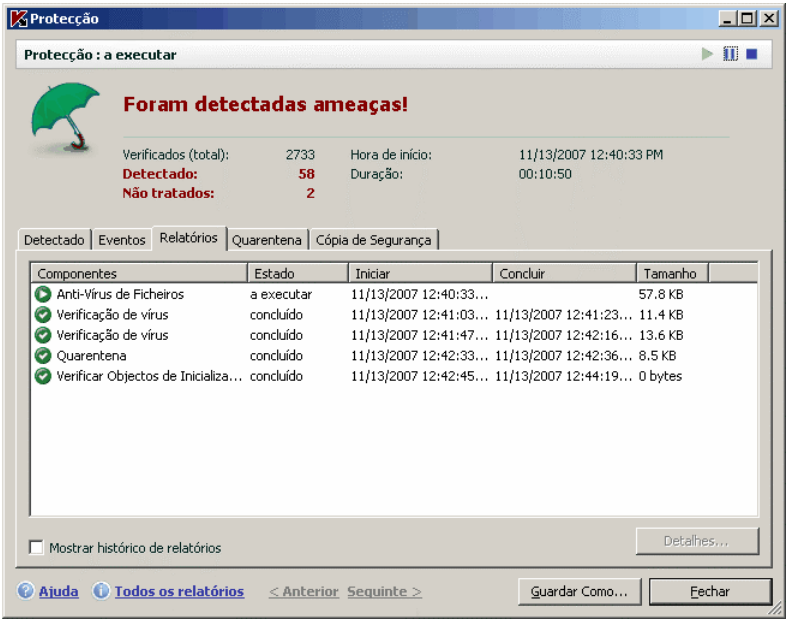


Figura 38. Relatórios sobre o funcionamento de componentes

Para rever todos os eventos gravados no relatório do Anti-Vírus de Ficheiros ou da tarefa:

Seleccione o Anti-Vírus de Ficheiros ou a tarefa no Separador **Relatórios** e clique no botão **Detalhes**.

Abrir-se-á uma janela com informação detalhada sobre o desempenho do Anti-Vírus de Ficheiros ou da tarefa seleccionada. As estatísticas de desempenho resultantes são exibidas na parte superior da janela e é fornecida informação detalhada nos vários separadores na parte central.

- O separador **Detectado** contém uma lista dos objectos perigosos detectados pelo Anti-Vírus de Ficheiros ou por uma tarefa de verificação de vírus executada.
- O separador **Eventos** exibe os eventos do Anti-Vírus de Ficheiros ou das tarefas.
- O separador **Estatísticas** contém estatísticas detalhadas para todos os objectos analisados.
- O separador **Definições** mostra as definições utilizadas pelo Anti-Vírus de Ficheiros, por verificações de vírus ou actualizações das assinaturas de ameaças.

- O separador **Utilizadores banidos** apresenta uma lista dos utilizadores cujos computadores foram banidos quando tentaram copiar ficheiros infectados ou potencialmente infectados para o servidor.

Pode exportar todo o relatório como um ficheiro de texto. Esta característica é útil nos casos onde ocorreu um erro no Anti-Vírus de Ficheiros, que você não pode eliminar sozinho e precisa da ajuda do Suporte Técnico. Se isto acontecer, o relatório deve ser enviado em formato .txt para o Suporte Técnico para que os nossos especialistas possam estudar o problema detalhadamente e resolvê-lo o mais rapidamente possível.

Para exportar um relatório como um ficheiro de texto:

Clique em **Guardar como** e especifique onde deseja guardar o ficheiro de relatório.

Quando acabar de trabalhar com o relatório, clique em **Fechar**.

Existe um botão Acções em todos os Separadores (excepto no separador **Definições** e **Estatísticas**) e que pode utilizar para definir respostas aos objectos na lista. Quando clica nele, abre-se um menu de contexto com os seguintes itens de menu (dependendo da componente, o menu difere – todas as opções possíveis estão listadas em baixo):

Desinfectar – tenta desinfectar um objecto perigoso. Se o objecto não for desinfectado com sucesso, pode deixá-lo nesta lista para o analisar mais tarde com novas actualizações ou apagá-lo. Pode aplicar esta acção a um único objecto da lista ou a vários objectos.

Apagar – apaga o registo da detecção do objecto do relatório.

Adicionar à Zona Confiável – exclui o objecto da protecção. Uma janela abrir-se-á com uma regra de exclusão para o objecto.

Ir para o Ficheiro – abre a pasta onde se encontra o objecto no Windows Explorer.

Neutralizar todos – neutraliza todos os objectos da lista. O Kaspersky Anti-Virus para Windows Servers tentará processar os objectos, utilizando as assinaturas de ameaças.

Descartar todos – esvazia o relatório dos objectos detectados. Ao utilizar esta função, todos os objectos perigosos detectados permanecem no seu computador.

Ver em www.viruslist.com – vai para uma descrição do objecto na Enciclopédia de Vírus da Kaspersky Lab.

Ver em www.google.com – encontra informação acerca do objecto, utilizando este motor de busca.

Procurar – introduz termos de pesquisa (por nome ou estado) para os objectos existentes na lista.

Além disso, pode ordenar a informação exibida na janela por ordem ascendente e descendente para cada uma das colunas, clicando no cabeçalho da coluna.

Para processar os objectos perigosos detectados pelo Kaspersky Anti-Virus, prima o botão **Desinfectar** (para um objecto ou um grupo de objectos seleccionados) ou **Neutralizar todos** (para processar todos os objectos na lista). Após cada objecto ser processado, aparecerá uma mensagem no ecrã. Aqui terá que decidir o que fazer com os objectos a seguir.

Se assinalar a opção ☑ **Aplicar a todos os casos semelhantes** na janela de notificação, a acção seleccionada será aplicada a todos os objectos com o mesmo estado seleccionados na lista antes de ter começado o processamento.

11.3.1. Configurar as definições dos relatórios

Para configurar definições para criar e guardar relatórios:

1. Abra a janela de definições do Kaspersky Anti-Virus para Windows Servers clicando em Definições na janela principal do programa.
2. Seleccione **Ficheiros de Dados** na árvore de definições.
3. Edite as definições na caixa **Relatórios** (ver Figura 39) como se segue:
   - Active ou desactive o registo de eventos informativos. Normalmente, estes eventos não são importantes para a segurança. Para registar eventos, seleccione ☑ **Registar eventos não críticos**;
   - Escolha apenas guardar eventos no relatório que ocorreram desde a última vez que a tarefa foi realizada. Isto poupa espaço no disco ao reduzir no tamanho do relatório. Se for seleccionada a opção ☑ **Guardar apenas eventos recentes**, a informação no relatório será actualizada todas as vezes que reiniciar a tarefa. No entanto, só a informação não crítica será apagada.
   - Configure o tempo de armazenamento para relatórios. Por definição, o tempo de armazenamento dos relatórios é de 90 dias, ao fim dos quais os relatórios serão apagados. Pode alterar o tempo máximo de armazenamento ou remover esta restrição.

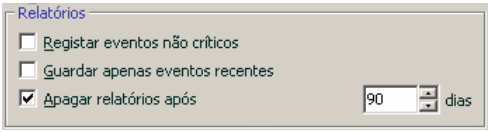


Figura 39. Configurar definições do relatório

11.3.2. Separador *Detectadas*

Este separador (ver Figura 40) contém uma lista dos ficheiros perigosos detectados pelo Kaspersky Anti-Virus para Windows Servers. É indicado o nome completo para cada ficheiro, juntamente com o estado atribuído pelo programa quando ele foi analisado e processado.

Se deseja que a lista contenha tanto os objectos perigosos, como os ficheiros neutralizados com sucesso, seleccione **Mostrar objectos neutralizados**.

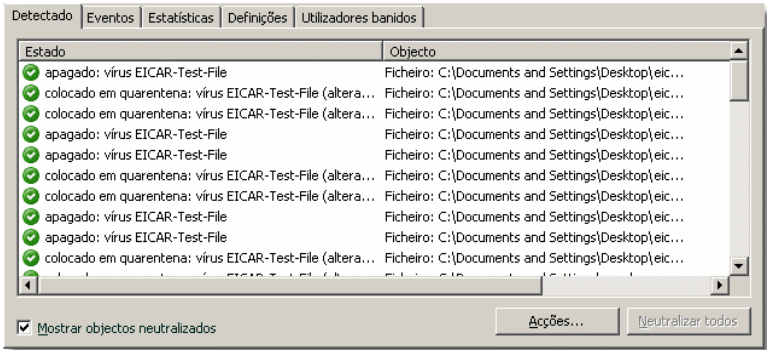


Figura 40. Lista dos objectos perigosos detectados

Os objectos perigosos detectados pelo Kaspersky Anti-Virus são processados, utilizando o botão **Neutralizar** (para um objecto ou um grupo de objectos seleccionados) ou **Neutralizar todos** (para processar todos os objectos na lista). Quando cada objecto for processado, aparecerá um aviso no ecrã, onde tem que decidir que acções serão tomadas a seguir.

Se assinalar a opção **Aplicar a todos os casos semelhantes** na janela de notificação, a acção seleccionada será aplicada a todos os objectos com o mesmo estado seleccionados na lista antes de ter começado o processamento.

11.3.3. Separador *Eventos*

Este separador (ver Figura 41) regista uma lista completa de todos os eventos importantes no funcionamento do Anti-Vírus de Ficheiros, verificações de vírus e actualizações das assinaturas de ameaças.

Os eventos podem ser:

Eventos críticos – são eventos de importância crítica que apontam para problemas no funcionamento do programa ou vulnerabilidades no seu computador. Por exemplo, *vírus detectado, erro na operação*.

Eventos importantes – são eventos que devem ser investigados, já que eles reflectem situações importantes no funcionamento do programa. Por exemplo, *parado.*

Mensagens informativas – são mensagens de referência tipo que geralmente não contêm informação importante. Por exemplo, *OK, não processado*. Estes eventos só se reflectem no registo de eventos se for seleccionada a opção ☑ **Mostrar todos os eventos**.

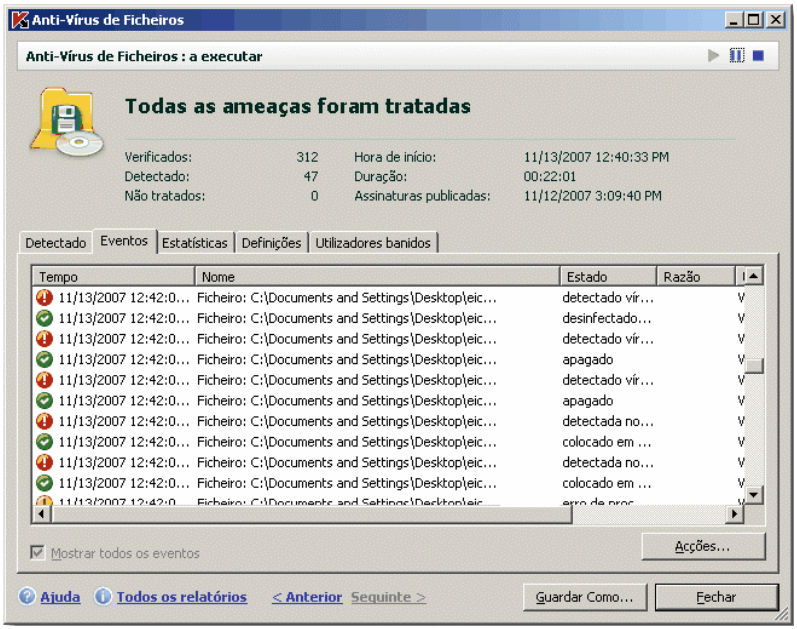

Anti-Vírus de Ficheiros
Anti-Vírus de Ficheiros : a executar
Todas as ameaças foram tratadas
Verificados: 312
Detectado: 47
Não tratados: 0
Hora de início: 11/13/2007 12:40:33 PM
Duração: 00:22:01
Assinaturas publicadas: 11/12/2007 3:09:40 PM
Detectado
Eventos
Estatísticas
Definições
Utilizadores banidos
Tempo
Nome
Estado
Razão
11/13/2007 12:42:0... Ficheiro: C:\Documents and Settings\Desktop\eic... detectado vír...
11/13/2007 12:42:0... Ficheiro: C:\Documents and Settings\Desktop\eic... desinfectado...
11/13/2007 12:42:0... Ficheiro: C:\Documents and Settings\Desktop\eic... detectado vír...
11/13/2007 12:42:0... Ficheiro: C:\Documents and Settings\Desktop\eic... apagado
11/13/2007 12:42:0... Ficheiro: C:\Documents and Settings\Desktop\eic... detectado vír...
11/13/2007 12:42:0... Ficheiro: C:\Documents and Settings\Desktop\eic... apagado
11/13/2007 12:42:0... Ficheiro: C:\Documents and Settings\Desktop\eic... detectada no...
11/13/2007 12:42:0... Ficheiro: C:\Documents and Settings\Desktop\eic... colocado em ...
11/13/2007 12:42:0... Ficheiro: C:\Documents and Settings\Desktop\eic... detectada no...
11/13/2007 12:42:0... Ficheiro: C:\Documents and Settings\Desktop\eic... colocado em ...
Mostrar todos os eventos
Acções...
Ajuda
Todos os relatórios
< Anterior
Seguinte >
Guardar Como...
Fechar

Figura 41. Eventos processados pela componente

O formato de exibição de eventos no registo de eventos pode variar em função da componente ou tarefa. É dada a seguinte informação para as tarefas de actualização:

- Nome do evento
- Nome do ficheiro envolvido no evento
- Hora a que o evento ocorreu
- Tamanho do ficheiro transferido

Para as tarefas de verificação de vírus, o registo do evento contém o nome do ficheiro analisado e o estado que lhe foi atribuído pela verificação/processamento.

11.3.4. Separador *Estatísticas*

Este separador (ver Figura 42) fornece-lhe estatísticas detalhadas sobre o Anti-Vírus de Ficheiros e sobre as tarefas de verificação de vírus. Aqui pode saber:

- Quantos objectos foram verificados nesta sessão do Anti-Vírus de Ficheiros ou depois de uma tarefa estar terminada. É exibido o número de arquivos analisados, ficheiros comprimidos, objectos protegidos por password e objectos corrompidos.
- Quantos objectos perigosos foram detectados, não desinfectados, apagados e colocados em Quarentena.

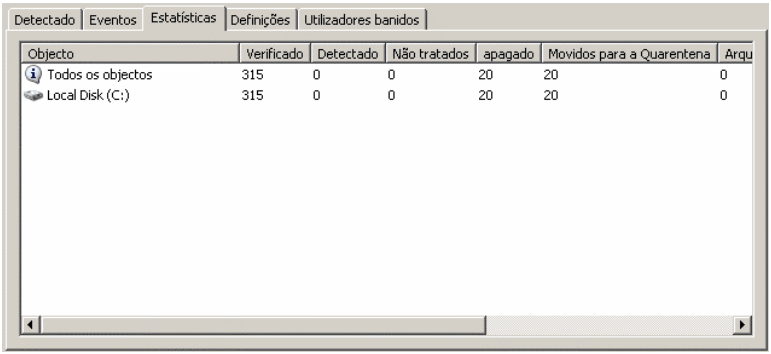


Figura 42. Estatísticas da componente

11.3.5. Separador *Definições*

O separador **Definições** (ver Figura 43) dá uma visão completa das definições do Anti-Vírus de Ficheiros, das verificações de vírus e das actualizações do programa. Pode descobrir em que nível estão a funcionar o Anti-Vírus de Ficheiros ou uma verificação de vírus, que acções estão a ser efectuadas com os ficheiros perigosos ou que definições estão a ser utilizadas para as actualizações do programa. Utilize a ligação Alterar definições para configurar a componente.

Pode configurar as definições avançadas para as verificações de vírus:

- Estabeleça a prioridade das tarefas de verificação utilizadas se o processador estiver muito pesado. Por defeito, a opção ☑ **Conceder recursos para outras aplicações** está assinalada. Com esta funcionalidade, o programa verifica a carga do processador e dos subsistemas do disco para a actividade de outras aplicações. Se a carga no processador aumentar significativamente e impedir as aplicações do utilizador de funcionarem normalmente, o programa reduzirá a actividade de verificação. Isto aumentará o tempo de verificação e libertará os recursos para as aplicações do utilizador.

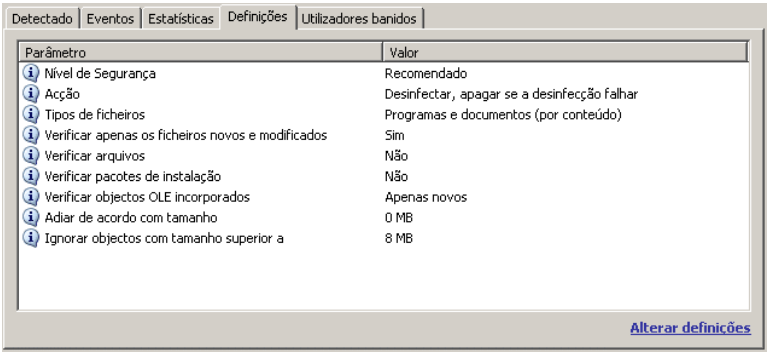


Figura 43. Definições da componente

- Configure o modo de funcionamento do servidor para depois da verificação de vírus estar completa. Pode configurar o servidor para se desligar, reiniciar ou entrar em modo de espera ou de economia de energia. Para seleccionar uma opção, clique com o botão esquerdo do rato na ligação até que esta mostre a opção que deseja.

11.3.6. Separador *Utilizadores banidos*

Todo o computador que tentou copiar um ficheiro infectado ou potencialmente infectado para o servidor é bloqueado (ver Figura 44). A proibição imposta sobre um computador também pode ser aplicado a acções relacionadas com o processamento do ficheiro (desinfecção ou eliminação).

Este separador diz-lhe que computadores foram banidos, juntamente com a data e hora a que isso ocorreu e quantas horas faltam até que deixem de estar banidos.

Figura 44. Lista de utilizadores banidos

11.4. Informação geral sobre o programa

Pode visualizar a informação geral sobre o programa na secção **Serviço** da janela principal (ver Figura 45).

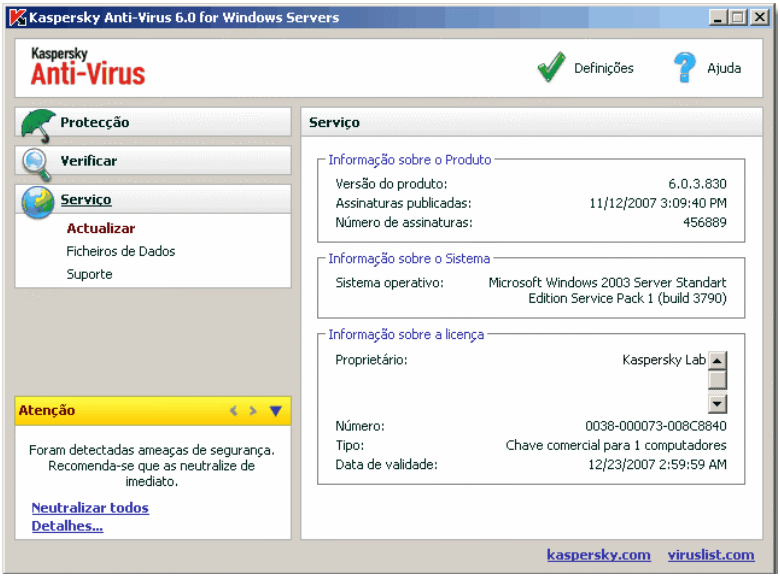


Figura 45. Informação sobre o programa, a licença e o sistema em que está instalado

Toda a informação está dividida em três secções:

- Na caixa **Informação sobre o Produto**, são exibidas as informações sobre a versão do programa, a data da última actualização e o número de ameaças conhecidas até à data.
- A informação básica sobre o sistema operativo instalado no seu computador está na caixa **Informação sobre o Sistema**.
- A informação básica sobre a licença que comprou para o Kaspersky Anti-Virus está na caixa **Informação sobre a licença**.

Precisará de toda esta informação ao contactar o Suporte Técnico da Kaspersky Lab (ver 11.6 na pág. 139).

11.5. Gerir licenças

O Kaspersky Anti-Virus para Windows Servers precisa de uma *chave de licença* para funcionar. Ser-lhe-á fornecida uma chave quando adquirir o programa. Esta chave dá-lhe o direito de utilizar o programa a partir do dia em que instala a chave.

Sem uma chave de licença, a não ser que tenha activado uma versão de avaliação da aplicação, o Kaspersky Anti-Virus funcionará no modo de uma actualização. O programa não transferirá nenhuma actualização nova.

Se tiver activado uma versão de avaliação do programa, após terminar o período de avaliação, o Kaspersky Anti-Vírus deixará de funcionar.

Quando a chave de licença comercial expira, o programa continua a trabalhar, mas não poderá fazer as actualizações das assinaturas de ameaças. Tal como anteriormente, poderá analisar o seu computador em termos de vírus e utilizar as componentes de protecção, mas só utilizando as assinaturas de ameaças que possuía quando a licença expirou. Não podemos garantir que fique protegido dos vírus depois da licença do programa expirar.

Para evitar a infecção do seu computador com novos vírus, recomendamos o prolongamento da sua licença do Kaspersky Anti-Virus para Windows Servers. O programa notificá-lo-á duas semanas antes da expiração da sua licença. O programa exibirá esta mensagens durante duas semanas de cada vez que o abrir.

Para renovar a licença, precisa de comprar e instalar uma nova chave de licença para a aplicação ou introduzir um código de activação da aplicação. Para o fazer:

Contacte o distribuidor onde comprou o produto e compre uma chave de licença da aplicação ou código da aplicação.

ou:

Obtenha uma chave de licença ou código de activação, directamente, na Kaspersky Lab, clicando na ligação Obter licença na janela da chave de licença (ver Figura 46). Complete o formulário no nosso site. Depois do pagamento ser efectuado, será enviado um link para o endereço de correio electrónico que introduziu no formulário de encomenda. Este link permitir-lhe-á transferir uma chave de licença da aplicação ou obter um código de activação.

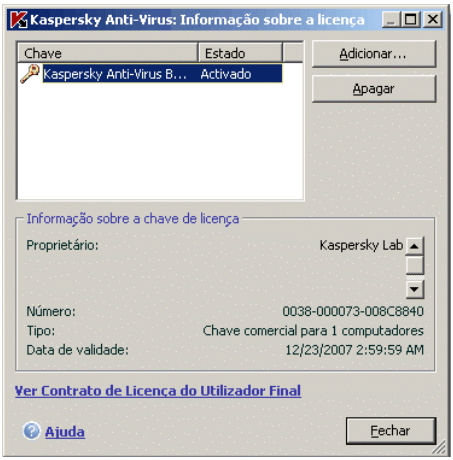


Figura 46. Informação sobre a licença

A Kaspersky Lab tem regularmente ofertas com preços especiais para os prolongamentos das licenças dos nossos produtos. Procure ofertas especiais no site da Kaspersky Lab em **Products → Sales and special offers**.

A informação acerca da chave de licença utilizada está disponível na caixa **Informação sobre a Licença** na secção **Serviço** da janela principal do programa. Para abrir a janela de gestor da licença, clique com o botão esquerdo do rato em qualquer lugar da caixa. Na janela que se abre (ver Figura 46), pode ver informação sobre a chave actual, adicionar uma chave ou apagar uma chave.

Quando selecciona uma chave na lista da caixa **Informação sobre a licença**, será apresentada informação sobre o número da licença, tipo de licença e data de validade da mesma. Para adicionar uma nova chave de licença, clique em **Adicionar** e active a aplicação com o assistente de activação (ver 11.5 na pág. 137). Para apagar uma chave da lista, utilize o botão **Apagar**.

Para rever os termos do CLUF, clique na ligação Ver Contrato de Licença do Utilizador Final. Para adquirir uma licença, utilizando o formulário da Internet no site da Kaspersky Lab, clique na ligação Comprar Licença.

11.6. Suporte Técnico

O Kaspersky Anti-Virus para Windows Servers fornece uma vasta gama de opções para as questões e problemas relacionados com o funcionamento do

programa. Estão todas localizadas na secção **Suporte** (ver Figura 47) em **Serviço**.

Dependendo do problema, oferecemos vários serviços de Suporte Técnico:

Fórum de Utilizadores. Este recurso é uma secção dedicada do site da Kaspersky Lab com perguntas, comentários e sugestões feitas pelos utilizadores do programa. Pode explorar os tópicos básicos do fórum e deixar um comentário seu. Também poderá encontrar a resposta à sua pergunta.

Para aceder a este recurso, utilize a ligação Fórum de Utilizadores.

Base de conhecimento. Este recurso também é uma secção dedicada do site da Kaspersky Lab e contém recomendações de Suporte Técnico para a utilização do software da Kaspersky Lab e respostas às perguntas mais frequentes. Tente encontrar uma resposta à sua pergunta ou uma solução para o seu problema através deste recurso.

Para obter Suporte Técnico online, utilize a ligação Base de Conhecimento.

Comentários sobre o funcionamento do programa. Este serviço está concebido para colocar comentários sobre o funcionamento do programa ou descrever um problema que surgiu durante o funcionamento do programa. Deve preencher um formulário especial no site da empresa que descreve, detalhadamente, a situação. De forma a tratar o problema da melhor maneira, a Kaspersky Lab necessitará de informação sobre o sistema. Poderá descrever a configuração do sistema ou utilizar o colector de informação automático no seu computador.

Para aceder ao formulário de comentários utilize a ligação Envie um relatório de erro ou uma sugestão.

Suporte Técnico. Se precisar de ajuda na utilização do Kaspersky Anti-Virus, clique na ligação existente na caixa **Suporte Técnico Local**. O site da Kaspersky Lab abrir-se-á com informação sobre como contactar os nossos especialistas.

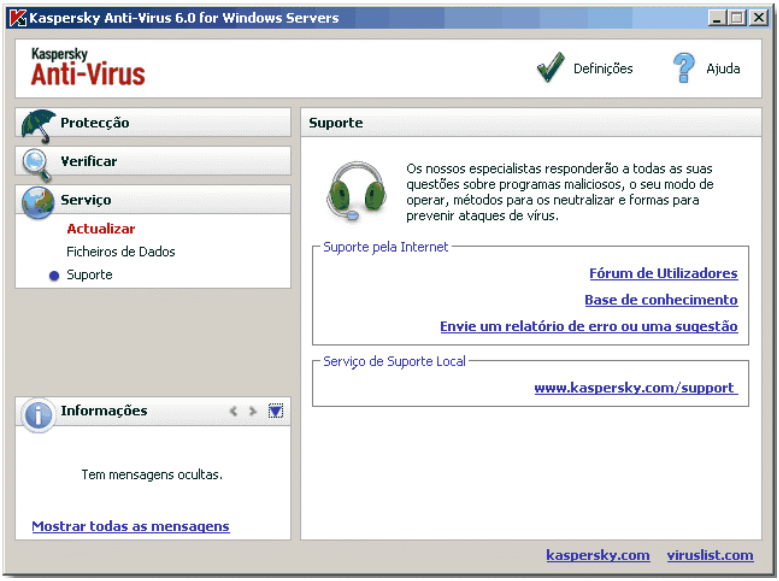


Figura 47. Informação sobre o Suporte Técnico

11.7. Configurar a Interface do Kaspersky Anti-Virus para Windows Servers

O Kaspersky Anti-Virus para Windows Servers dá-lhe a opção de alterar o aspecto do programa, criando e utilizando máscaras. Você também pode configurar a utilização de elementos de interface activos tais como o ícone de bandeja do sistema e as mensagens de popup.

Para configurar a interface do programa, siga os passos seguintes:

1. Abra a janela de definições do Kaspersky Anti-Virus para Windows Servers clicando na ligação Definições na janela principal.
2. Seleccione **Aparência** na secção **Serviço** da árvore de definições do programa (ver Figura 48).

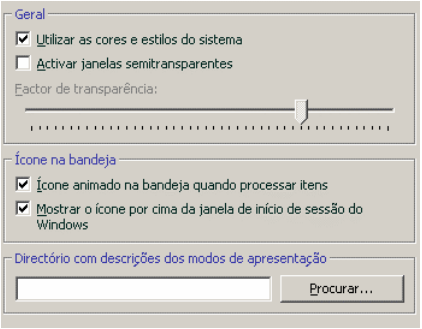

Geral
Utilizar as cores e estilos do sistema
Activar janelas semitransparentes
Factor de transparência:
Ícone na bandeja
Ícone animado na bandeja quando processar itens
Mostrar o ícone por cima da janela de início de sessão do Windows
Directório com descrições dos modos de apresentação
Procurar...

Figura 48. Configurar as definições da interface do programa

Na parte direita da janela de definições você pode determinar:

- Se apresenta o indicador de protecção do Kaspersky Anti-Virus para Windows Servers quando o sistema operativo se inicia.

  Este indicador aparece por definição no canto superior direito do ecrã quando o programa se inicia. Ele informa-o que o seu computador está protegido contra todos os tipos de ameaças. Se não deseja utilizar o indicador de protecção, retire a selecção em ☑ **Mostrar o ícone por cima da janela de inicio de sessão do Windows**.

- Se utiliza animação no ícone da barra do sistema.

  Dependendo da operação do programa efectuada, o ícone da bandeja do sistema altera-se. Por defeito, a animação do ícone é utilizada. Se deseja desactivar a animação, desmarque a opção ☑ **Ícone animado na bandeja quando processar itens**. Então o ícone só reflectirá o estado de protecção do seu computador: se a protecção estiver activada, o ícone está a cores, e se a protecção estiver suspensa ou desactivada, o ícone será cinzento.

- Grau de transparência das mensagens de popup.

  Todas as operações do Kaspersky Anti-Virus para Windows Servers que devam chegar imediatamente até si ou que necessitem da sua decisão são apresentadas como mensagens de popup sobre o ícone bandeja do sistema. As janelas da mensagem são translúcidas de forma a não interferirem com outras operações. Se mover o cursor por cima da mensagem, a transparência desaparece. Você pode ajustar o grau de transparência dessas mensagens. Para o fazer, ajuste a escala **Factor de transparência** para a posição desejada. Para remover a transparência das mensagens, desmarque a opção ☑ **Activar janelas semitransparentes**.

- Utilize os seus próprios modos de apresentação para a interface do programa.

  Todas as cores, fontes, ícones e textos utilizados na interface do Kaspersky Anti-Virus para Windows Servers podem ser alteradas. Você pode criar os seus próprios gráficos para o programa ou pode colocá-lo numa outra linguagem. Para utilizar um modo de apresentação, especifique o directório com as suas definições no campo **Directório com descrições dos modos de apresentação**. Utilize o botão **Procurar** para seleccionar o directório.

  Por definição, as cores do sistema e os estilos são utilizados no modo de apresentação. Pode removê-los, desmarcando a opção ☑ **Utilizar as cores e estilos do sistema**. Então, serão utilizados os estilos que você especificou nas definições do tema de ecrã.

Repare que as alterações à interface do Kaspersky Anti-Virus não são guardadas se restaurar as predefinições ou desinstalar o programa.

11.8. Utilizar as opções avançadas

O Kaspersky Anti-Virus para Windows Servers fornece-lhe as seguintes funcionalidades avançadas:

- Notificações de determinados eventos que ocorrem no programa.
- A Autodefesa do Kaspersky Anti-Virus para Windows Servers no que respeita a módulos a desactivar, apagar ou editar, assim como a protecção por password para o programa.
- Resolução de conflitos entre o Kaspersky Anti-Virus e outros programas.

Para configurar estas funções:

1. Abra a janela de configuração do programa através da ligação Definições na janela principal.
2. Seleccione a secção **Serviço** a partir da árvore de definições.

Na parte direita do ecrã, pode definir se utilizará funcionalidades adicionais no funcionamento do programa.

11.8.1. Notificações de eventos do Kaspersky Anti-Virus para Windows Servers

Ocorrem diferentes tipos de eventos no Kaspersky Anti-Virus para Windows Servers. Podem ser de natureza informativa ou conter informação importante. Por exemplo, um evento pode informá-lo de que o programa se actualizou com sucesso ou pode guardar um erro na componente que deve ser imediatamente eliminado.

Para receber notificações sobre o funcionamento do Kaspersky Anti-Virus para Windows Servers, pode utilizar a funcionalidade de notificação.

Os avisos podem ser entregues de diversas formas:

- Mensagens de popup por cima do ícone do programa na barra do sistema
- Mensagens sonoras
- Mensagens de e-mail
- Registo de eventos

Para utilizar esta funcionalidade, deve:

1. Seleccionar a opção ☑ **Activar notificações** na caixa **Interacção com o utilizador** (ver Figura 49).

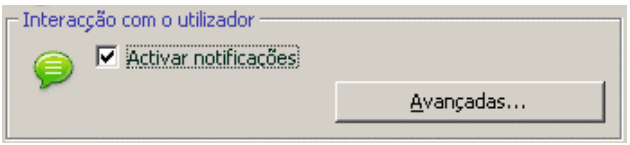


Figura 49. Activar notificações

2. Definir os tipos de eventos do Kaspersky Anti-Virus para Windows Servers, dos quais pretende notificações e o método de entrega da notificação (ver 11.8.1.1 na pág. 145).
3. Configurar as definições de entrega de notificações por e-mail, se esse for o método que está a ser utilizado (ver 11.8.1.2 na pág. 146).

11.8.1.1. Tipos de eventos e métodos de entrega das notificações

Durante o funcionamento do Kaspersky Anti-Virus para Windows Servers, surgem os seguintes tipos de eventos:

Notificações críticas são eventos de uma importância crítica. As notificações são altamente recomendadas, já que apontam problemas no funcionamento do programa ou vulnerabilidades na protecção do seu computador. Por exemplo, *assinaturas de ameaça corrompidas ou licença expirada*.

Falha funcional – eventos que levam a que o programa não funcione. Por exemplo, *sem licença ou assinaturas de ameaças*.

Notificações importantes são eventos que devem ser investigados, já que reflectem situações importantes no funcionamento do programa. Por exemplo, *protecção desactivada ou o computador não é analisado há muito tempo.*

Notificações menores são mensagens referência - tipo que geralmente não contêm informação importante. Por exemplo, *todos os ficheiros perigosos estão desinfectados*.

Para especificar sobre que eventos o programa o deveria notificar e como:

1. Clique na ligação Definições na janela principal do programa.
2. Na janela de definições do programa, seleccione **Serviço**, assinale a opção ☑ **Activar notificações** e edite as definições detalhadas, clicando no botão **Avançadas**.

Você pode configurar os seguintes métodos de notificação para os eventos acima listados na janela **Definições de notificação** que se abre (ver Figura 50):

- *Mensagens de popup* por cima do ícone do programa na barra do sistema, que contêm uma mensagem informativa sobre o evento que aconteceu.

  Para utilizar este tipo de notificação, seleccione ☑ **Balão** à frente do evento sobre o qual deseja ser informado.

- *Notificação sonora*

  Se deseja que esta notificação seja acompanhada por um ficheiro de som, seleccione ☑ **Som** à frente do evento.

- *Notificação por mensagem de correio electrónico*

Para utilizar este tipo de notificação, assinale a coluna **E-mail** à frente do evento sobre o qual deseja ser informado e configure as definições para envio de notificações (ver 11.8.1.2 na pág. 146).

- *Registo de eventos*

  Para registar informação no registo sobre qualquer evento que ocorra, assinale a caixa à frente do evento na coluna **Log** e configure as definições do log do evento (ver 11.8.1.3 na pág. 147).

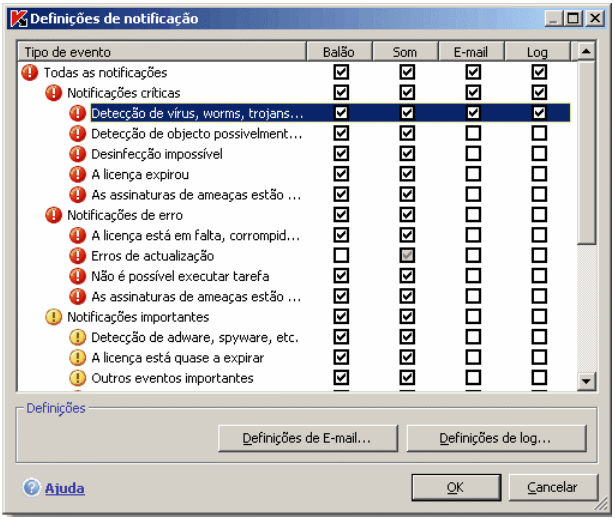


Figura 50. Eventos do programa e métodos de notificação de eventos

11.8.1.2. Configurar notificações por e-mail

Depois de ter seleccionado os eventos (ver 11.8.1.1 na pág. 145) acerca dos quais deseja receber notificação por e-mail, deve configurar a entrega da notificação. Para o fazer:

1. Abra a janela de configuração do programa com a ligação Definições na janela principal.
2. Seleccione **Serviço** na árvore de definições.
3. Clique em **Avançadas** na caixa **Interacção com o utilizador**.
4. No separador **Definições de notificação**, seleccione a caixa de selecção na coluna **E-mail** para os eventos que devem gerar uma mensagem de e-mail.

5. Na janela que se abre quando clica em **Definições de E-mail**, configure as seguintes definições para enviar notificações por e-mail:

   - Atribua a definição de envio de notificação em **De**: **Endereço de e-mail**.

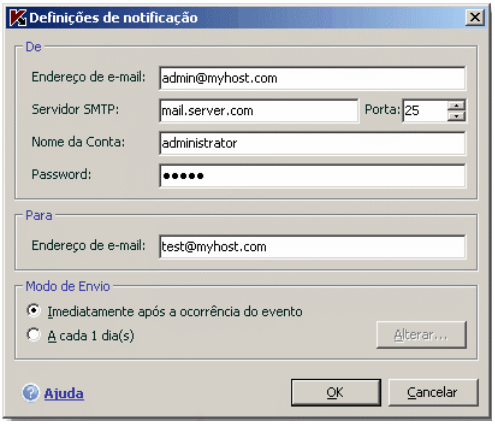


Figura 51. Configurar definições de notificação por e-mail

   - Especifique o endereço de e-mail para o qual serão enviadas as notificações em **Para: Endereço de e-mail**.

   - Atribua um método de entrega da notificação por e-mail em **Modo de Envio**. Se deseja que o programa envie um e-mail assim que o evento ocorrer, seleccione a opção **Imediatamente após a ocorrência do evento**. Para as notificações sobre eventos com um certo período de tempo, preencha o agendamento para envio de e-mails informativos, clicando em **Alterar**. A predefinição são as notificações diárias.

11.8.1.3. Configurar definições de registo de eventos

Para configurar as definições do registo de eventos:

1. Abra a janela de configuração do programa com a ligação Definições na janela principal.
2. Seleccione **Serviço** na árvore de definições.
3. Clique em **Avançadas** na secção **Interacção com o utilizador** na parte direita do ecrã.

Na janela de **Definições de notificação**, seleccione a opção para registar informação para um evento e clique no botão **Definições de log**.

O Kaspersky Anti-Virus tem a opção de guardar informação acerca de eventos que ocorram enquanto o programa está a funcionar, quer no registo de eventos geral do Microsoft Windows (**Aplicação**) ou num registo de eventos dedicado do Kaspersky Anti-Virus (**Log de Eventos da Kaspersky**).

Os registos podem ser visualizados no **Visualizador de eventos** do Microsoft Windows, que pode abrir acedendo a **Iniciar → Painel de Controlo → Ferramentas Administrativas → Visualizador de Eventos**.

11.8.2. Autodefesa e restrição de acesso

O Kaspersky Anti-Virus para Windows Servers garante a segurança do seu computador contra programas maliciosos, e por esse facto, ele pode ser o alvo de programas maliciosos que tentam bloquear o programa ou mesmo apagá-lo no computador.

Cada vez mais várias pessoas podem utilizar um PC, todas com níveis variados de conhecimento sobre computadores. Deixar aberto o acesso ao programa e às suas definições pode baixar, dramaticamente, a segurança do computador como um todo.

Para assegurar a estabilidade do sistema de segurança do seu computador, a Autodefesa, defesa de acesso remoto e os mecanismos de protecção por password foram adicionados ao programa.

Para activar a Autodefesa:

1. Abra a janela de definições do programa através da ligação Definições na janela principal.
2. Seleccione **Serviço** na árvore de definições.

Defina as seguintes configurações na caixa **Autodefesa** (ver Figura 52):

- ☑ **Activar Autodefesa**. Se esta caixa for seleccionada, o programa protegerá os seus próprios ficheiros, processos na memória e entradas no registo do sistema, impedindo-os de serem apagados ou modificados.
- ☑ **Desactivar Serviço de Controle Externo**. Se esta caixa for seleccionada, qualquer programa de administração remota que tente utilizar o programa será bloqueado.

Se alguma das acções listadas forem tentadas, aparecerá uma mensagem por cima do ícone do programa na barra do sistema (a não ser que o utilizador tenha desactivado as notificações).

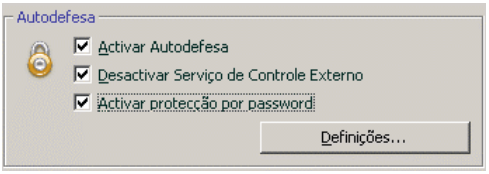


Figura 52. Configurar defesa do programa

Para proteger o programa através de uma password, seleccione **Activar protecção por password**. Clique no botão **Definições** para abrir a janela **Protecção por password** e introduza a password e a área que a restrição de acesso abrangerá (ver Figura 53).

Figura 53. Definições da protecção por password do programa

Pode bloquear qualquer operação do programa, excepto as notificações de detecção de objectos perigosos ou evitar que alguma das seguintes acções seja efectuada:

- Alteração das definições de funcionamento do programa
- Encerramento do Kaspersky Anti-Virus para Windows Servers
- Desactivação ou pausa da protecção do seu computador

Cada uma destas acções diminui o nível de protecção do servidor, por isso tem que definir as pessoas que irão trabalhar com o servidor.

Agora, sempre que um utilizador tentar efectuar as acções que você seleccionou no servidor, o programa pedirá uma password.

11.8.3. Resolver conflitos com outras aplicações

Nalguns casos, o Kaspersky Anti-Virus pode causar conflitos com outras aplicações instaladas no computador. Isso acontece porque esses programas têm mecanismos integrados de autodefesa que se activam quando o Kaspersky Anti-Virus tenta inspeccioná-los. Estas aplicações incluem o plug-in Authentica para o Acrobat Reader, que verifica o acesso a ficheiros .pdf, o Oxygen Phone Manager II e alguns jogos de computador que têm ferramentas de gestão de direitos digitais.

Para corrigir este problema, assinale a opção ☑ **Modo de compatibilidade para programas através de métodos de autoprotecção** na secção **Serviço** da janela de definições da aplicação. Tem que reiniciar o seu sistema operativa para que esta alteração entre em efeito.

11.9. Importar e exportar as definições do Kaspersky Anti-Virus para Windows Servers

O Kaspersky Anti-Virus para Windows Servers permite-lhe importar e exportar as suas próprias definições.

As definições são guardadas num ficheiro especial de configuração.

Para exportar as actuais definições do programa:

1. Abra a janela principal do Kaspersky Anti-Virus para Windows Servers.
2. Seleccione a secção **Serviço** e clique em Definições.
3. Clique no botão **Guardar** na secção **Gestor de configuração**.
4. Insira um nome para o ficheiro de configuração e seleccione um destino para o guardar.

Para importar as definições a partir de um ficheiro de configuração:

1. Abra a janela principal do Kaspersky Anti-Virus para Windows Servers.
2. Seleccione a secção **Serviço** e clique em Definições.
3. Clique no botão **Carregar** e seleccione o ficheiro a partir do qual pretende importar as definições do Kaspersky Anti-Virus para Windows Servers.

11.10. Repor as predefinições

É sempre possível repor as predefinições do programa, que são consideradas óptimas e são recomendadas pela Kaspersky Lab. Isso pode ser feito utilizando o Assistente de Configuração.

Para repor as definições da protecção:

1. Seleccione a secção **Serviço** e clique em Definições para aceder à janela de configuração do programa.
2. Clique no botão **Restaurar** na secção **Gestor de configuração**.

A janela que se abre pede-lhe para especificar que definições devem ser restauradas para os seus valores predefinidos.

Por defeito, o programa guarda todas as definições personalizadas na lista (por defeito, elas estão desmarcadas). Se não precisar de guardar uma destas definições, assinale a caixa correspondente que surge antes da mesma.

Depois de terminar de configurar as definições, clique no botão **Seguinte** (ver 3.2 na pág. 28). O Assistente de Configuração irá abrir-se. Siga as instruções deste assistente.

Quando você terminar o Assistente de Configuração, o nível de segurança **Recomendado** será definido para o Anti-Vírus de Ficheiros, excepto para as definições que você decidiu guardar. Para além disso, as definições, com as quais configurou o Assistente de Configuração, também serão aplicadas.

CAPÍTULO 12. ADMINISTRAR O PROGRAMA COM O KASPERSKY ADMINISTRATION KIT

O **Kaspersky Administration Kit** é um sistema para gerir, de forma centralizada, as tarefas administrativas com chaves na operação de um sistema de segurança para uma rede empresarial, com base nas aplicações incluídas nas soluções Kaspersky Anti-Virus Business Optimal e Kaspersky Corporate Suite.

O Kaspersky Anti-Virus 6.0 para Windows Servers é um dos produtos da Kaspersky Lab que pode ser administrado através da sua própria interface, a linha de comandos (estes métodos são descritos acima nesta documentação) ou através do Kaspersky Administration Kit (se o computador fizer parte do sistema centralizado de administração remota).

Execute os seguintes passos para gerir o Kaspersky Anti-Virus 6.0 para Windows Servers através do Kaspersky Administration Kit:

- Instale o *Servidor de Administração* na rede; instale a *Consola de Administração* no local de trabalho do administrador (para mais detalhes, veja o Manual de Utilização do Administrador para implementação do Kaspersky Administration Kit);
- Nos servidores de ficheiros da rede, instale o Kaspersky Anti-Virus 6.0 para Windows Servers e *NAgent* (incluído com o Kaspersky Administration Kit) em computadores da rede. Para mais detalhes sobre a instalação remota do Kaspersky Anti-Virus em computadores da rede, veja o Guia do Administrador para implementação do Kaspersky Administration Kit 6.0.

Depois de actualizar a extensão de administração da Kaspersky Lab através do Kaspersky Administration Kit, encerre a Consola de Administração.

A *Consola de Administração* (ver Figura 54) permite-lhe administrar a aplicação através do Kaspersky Administration Kit. É uma **Interface Integrada MMC** (Consola de Administração da Microsoft) padrão e permite ao administrador executar as seguintes funções:

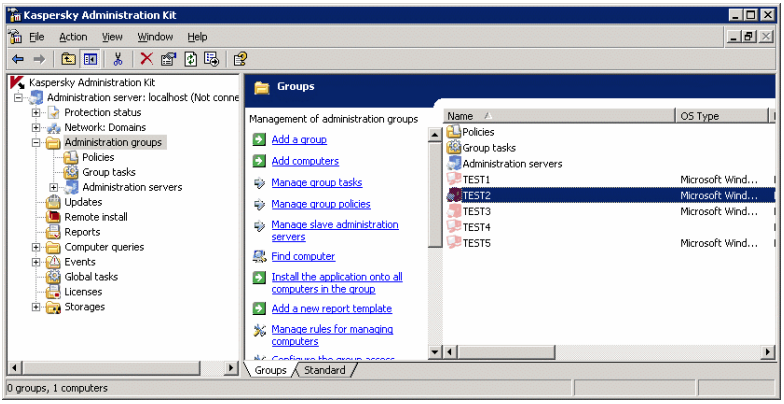


Figura 54. Consola de Administração do Kaspersky Administration Kit

- Instalar de forma remota o Kaspersky Anti-Virus 6.0 para Windows Servers e *NAgent* em computadores da rede
- Configurar de forma remota o Kaspersky Anti-Virus em computadores da rede
- Actualizar as assinaturas de ameaças e módulos do Kaspersky Anti-Virus
- Gerir licenças para a aplicação em computadores da rede
- Ver informação acerca do funcionamento do programa em computadores cliente

Quando trabalhar através do Kaspersky Administration Kit, o programa é administrado por definições de política, definições de tarefa e definições da aplicação definidas pelo administrador.

As **Definições da Aplicação** são um conjunto de definições para o funcionamento do programa, incluindo definições de protecção geral, definições da Cópia de Segurança e da Quarentena, definições da produção de relatórios, etc.

A **Tarefa** é uma acção específica executada pela aplicação. As tarefas do Kaspersky Anti-Virus para Windows Servers são divididas por tipo, de acordo com a função (tarefas de verificação de vírus, tarefas de actualização do programa, reversão de actualização e tarefas de instalação de chaves de licença). Cada tarefa específica tem um conjunto de definições do Kaspersky Anti-Virus que são usadas quando a tarefa é executada *(definições da tarefa)*.

A função-chave da administração centralizada é o agrupamento de computadores remotos e a gestão das suas definições através da criação e configuração de políticas de grupo.

Uma **Política** é um grupo de definições para o funcionamento do programa em computadores em grupos de trabalho em rede, assim como grupos de restrições à reconfiguração dessas definições ao configurar a aplicação e tarefas num computador cliente individual.

Uma política inclui definições para a configuração de todas as funções do programa. Desse modo, as políticas incluem as definições do programa e definições para todos os tipos de tarefas, excepto as definições específicas de um determinado tipo de tarefa.

12.1. Administrar a aplicação

O Kaspersky Administration Kit dá-lhe a oportunidade de parar e pausar, de forma remota, o Kaspersky Anti-Virus em computadores clientes individuais, assim como configurar definições gerais para a aplicação, tais como a activação/desactivação da protecção do computador, a configuração de definições da Cópia de Segurança e Quarentena e a configuração de definições para a produção de relatórios.

Para gerir as definições da aplicação:

1. Seleccione a pasta do grupo que contém o computador cliente na pasta **Grupos** (ver Figura 54).
2. Na janela que se abre, seleccione o computador para o qual você precisa de modificar as definições da aplicação. No menu de contexto ou no menu **Acções**, seleccione o comando **Propriedades**.
3. O separador **Aplicações** na janela de propriedades do computador cliente (ver Figura 55) apresenta uma lista completa das aplicações da Kaspersky Lab instaladas no computador cliente.

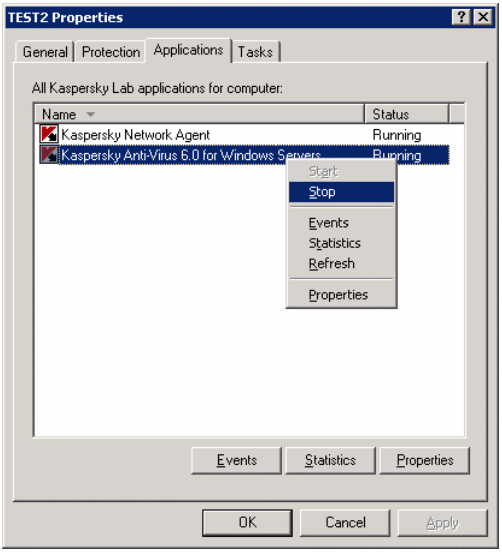


Figura 55. Lista de aplicações da Kaspersky Lab

Existem botões de controlo por baixo da lista de programas, os quais pode utilizar para:

- Ver uma lista de eventos no funcionamento da aplicação que ocorreram no cliente e que foram guardadas no Servidor de Administração
- Ver estatísticas actuais sobre o funcionamento do programa
- Configurar as definições do programa (ver 12.1.2 na pág. 156)

12.1.1. Iniciar/parar a aplicação

Pode iniciar ou pausar o Kaspersky Anti-Virus num computador remoto, utilizando os comandos do menu de contexto na janela de propriedades do computador (ver Figura 55).

Pode executar as mesmas acções, utilizando os botões **Iniciar/Parar** a partir da janela de definições no separador **Geral** (ver Figura 56).

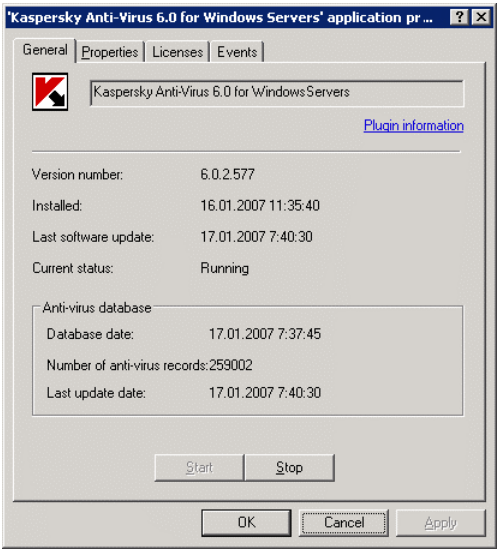


Figura 56. Configurar as definições do Kaspersky Anti-Virus. Separador **Geral**

Na parte superior da janela, vai encontrar o nome da aplicação instalada, informação sobre a versão, a data de instalação, o seu estado (se a aplicação está em execução ou pausada no computador local) e informação acerca do estado da base de dados de assinaturas de ameaças.

12.1.2. Configurar as definições da aplicação

Para ver ou alterar as definições da aplicação:

1. Abra a janela de propriedades para o computador cliente no separador **Aplicações** (ver Figura 54).
2. Seleccione o **Kaspersky Anti-Virus 6.0 para Windows Servers**. Clique no botão **Propriedades** para abrir a janela de definições da aplicação.

Todos os separadores, com excepção do separador **Propriedades,** são separadores padrão para o Kaspersky Administration Kit. Para mais informação sobre os separadores padrão, veja o Guia do Administrador.

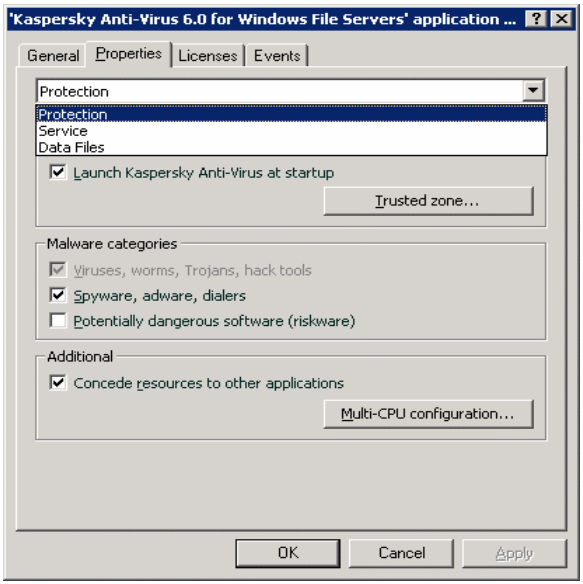


Figura 57. Configurar as definições do Kaspersky Anti-Virus.
Separador **Propriedades**

Se tiver sido criada uma política para a aplicação (ver 12.3.1 na pág. 166) que impede que algumas definições sejam reconfiguradas, estas não serão editáveis ao configurar a aplicação.

No separador **Definições**, pode configurar as definições gerais e de serviço para a protecção do Kaspersky Anti-Virus, definições da Cópia de Segurança e Quarentena e definições para a produção de relatórios. Para o fazer, seleccione o valor necessário do menu suspenso na parte superior da janela e configure as definições:

Protecção
Nesta janela, você pode: • Activar/desactivar a protecção para um computador (ver 6.1 na pág. 55) • Configurar a inicialização automática para a aplicação quando o computador for ligado (ver 6.1.5 na pág. 59) • Criar uma zona confiável ou uma lista de exclusões (ver 6.3 na pág. 60) • Seleccionar os tipos de programas maliciosos que a aplicação irá

monitorizar (ver 6.2 na pág. 59) • Configurar definições de produtividade para a aplicação e definições de configuração multi-processador (ver 6.7 na pág. 71)
Serviço
A configuração de definições de serviço inclui: • Configurar notificações para eventos que ocorram (ver 11.8.1 na pág. 144) • Gerir a função de auto-defesa da aplicação e a protecção das definições da aplicação através de password (ver 11.8.2 na pág. 148) • Configurar a aparência da aplicação (ver 12.3.1 na pág. 166) • Configurar definições de compatibilidade entre o Kaspersky Anti-Virus e outros programa (ver 11.8.3 na pág. 150)
Ficheiros de Dados
Nesta janela, pode configurar as definições para a produção de estatísticas de relatório sobre o funcionamento do programa (ver 11.3.1 na pág. 131) e especificar o tempo durante o qual os ficheiros são armazenados na Cópia de Segurança (ver 11.2.2 na pág. 126) e na Quarentena (ver 11.1.2 na pág. 123).

12.1.3. Configurar definições específicas

Quando administra o Kaspersky Anti-Virus através do Kaspersky Administration Kit, pode activar/desactivar a interactividade e editar a informação sobre o Suporte Técnico. Para o fazer:

1. Abra a janela de propriedades para o computador cliente no separador **Aplicações** (ver Figura 55).
2. Seleccione o **Kaspersky Anti-Virus 6.0 para Windows Servers** e use o botão **Propriedades**. Como resultado, abrir-se-á uma janela de definições da aplicação (ver Figura 57). Seleccione **Serviço** a partir do menu suspenso na parte superior da janela.

No separador **Serviço** da secção **Aparência**, pode activar/desactivar a interactividade do Kaspersky Anti-Virus num computador remoto: a apresentação do ícone do Kaspersky Anti-Virus na bandeja do sistema, a emissão de notificações sobre eventos ocorridos na aplicação (por exemplo, a detecção de um objecto perigoso).

Se a opção **Permitir interactividade** estiver assinalada, um utilizador que estiver a trabalhar num computador remoto verá o ícone e mensagens de pop-up do Anti-Virus e terá a capacidade para tomar decisões sobre os passos subsequentes a tomar nas janelas de notificação em relação a eventos que ocorram. Para desactivar a interactividade da aplicação, desmarque a caixa de selecção.

No separador **Informação de suporte personalizada,** na janela que se abre quando clica no botão **Definições**, pode editar a informação sobre o suporte técnico do utilizador, que é fornecida na secção **Serviço** do item **Suporte** do Kaspersky Anti-Virus (ver Figura 47).

Para alterar a informação no campo superior, introduza o texto actual sobre o suporte fornecido. No campo que surge por baixo, pode editar as hiperligações que são apresentadas na caixa **Suporte Técnico Online**, que se abre quando selecciona **Suporte** na secção **Serviço**.

Você pode editar a lista de origens, utilizando os botões **Adicionar**, **Editar** e **Apagar**. O Kaspersky Anti-Virus irá adicionar um novo link ao topo da lista. Para alterar a ordem dos links na lista, use os botões **Mover cima**/**Mover baixo**.

Se a janela não contiver nenhum dado, a informação predefinida sobre o suporte técnico não está sujeita a edição.

12.2. Gerir tarefas

Esta secção inclui informação sobre como gerir tarefas para o Kaspersky Anti-Virus 6.0 para Windows Servers. Para mais informação sobre o conceito de gestão de tarefas através do Kaspersky Administration Kit 6.0, veja o Guia do Administrador para o programa.

Quando a aplicação é instalada, é criado um conjunto de tarefas de sistema para cada computador. Esta lista (ver Figura 58) inclui tarefas de protecção em tempo real (Anti-Vírus de Ficheiros), tarefas de verificação de vírus (O Meu Computador, Objectos de Inicialização, Áreas Críticas) e tarefas de actualização (actualizações de assinaturas de ameaças e dos módulos da aplicação, reversão de actualizações e distribuição de actualizações).

Você pode iniciar tarefas de sistema e configurar definições e agendamentos para as mesmas, mas as mesmas não podem ser apagadas.

Para além disso, você pode criar as suas próprias tarefas, tais como verificações de vírus, actualizações da aplicação, reversão de actualizações e tarefas de instalação de chaves de licença.

Para ver uma lista das tarefas criadas para um computador cliente:

1. Seleccione a pasta do grupo que contém o computador cliente na pasta **Grupos** (ver Figura 54).
2. Na janela que se abre, seleccione o computador para o qual você precisa de criar uma tarefa local e use o comando **Tarefas** no menu de contexto ou o mesmo comando no menu **Acções**. De seguida, na janela principal abrir-se-á uma janela com as propriedades do computador cliente.
3. O separador **Tarefas** (ver Figura 58) apresenta uma lista completa das tarefas criadas para aquele computador cliente.

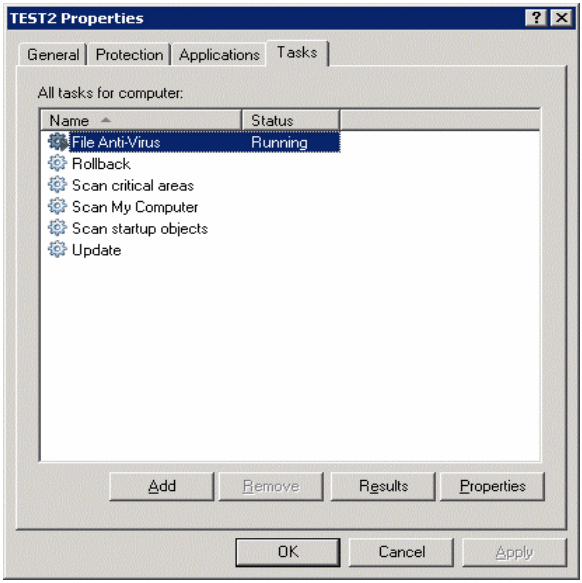


Figura 58. Lista de tarefas das aplicações

12.2.1. Iniciar e parar tarefas

As tarefas são iniciadas no computador cliente apenas se a aplicação correspondente estiver a funcionar (ver 12.1.1 na pág. 155). Se a aplicação estiver parada, todas as tarefas serão terminadas.

As tarefas são iniciadas e pausadas automaticamente, de acordo com um agendamento, ou manualmente, utilizando os comandos a partir do menu de

contexto e a partir da janela Ver Definições da Tarefa. Também pode pausar tarefas e retomá-las.

Para iniciar/parar/pausar/retomar uma tarefa manualmente:

Seleccione a tarefa necessária a partir da janela de resultados, abra o menu de contexto e seleccione **Iniciar/Parar/Pausar/Retomar** ou use os mesmos comandos no menu **Acções**.

Pode iniciar operações similares a partir da janela de definições da tarefa no separador **Geral** (ver Figura 59), ao utilizar os botões correspondentes.

12.2.2. Criar tarefas

Ao trabalhar com a aplicação através do Kaspersky Administration Kit, você pode criar:

- Tarefas locais, configuradas para computadores individuais
- Tarefas de grupo, configuradas para computadores unidos num grupo da rede
- Tarefas globais, configuradas para qualquer conjunto de computadores de qualquer grupo da rede

Você pode alterar as definições de tarefas, monitorizar o seu desempenho, copiar e mover tarefas de um grupo para outro e também apagá-las, utilizando os comandos padrão **Copiar/Colar**, **Cortar/Colar** e **Apagar** a partir do menu de contexto ou os mesmos comandos a partir do menu **Acções**.

12.2.2.1. Criar tarefas locais

Para criar uma tarefa local, siga os seguintes passos:

1. Abra a janela de propriedades para o computador cliente no separador **Tarefas** (ver Figura 58).
2. Use o botão **Adicionar** para adicionar uma nova tarefa. Isso abrirá uma janela Criar Nova Tarefa, que é concebida como um Assistente padrão do Windows e consiste numa série de passos e você pode navegar entre eles utilizando os botões **Anterior** e **Seguinte** ou finalizar com o botão **Concluir**. O botão **Cancelar** irá parar o processo em qualquer ponto.

Passo 1. Introduzir dados gerais na tarefa

A primeira janela principal é introdutória: aqui deve especificar o nome da tarefa (o campo **Nome**).

Passo 2. Seleccionar uma aplicação e tipo de tarefa

Neste passo, deve especificar a aplicação para a qual está a ser criada a tarefa (Kaspersky Anti-Virus 6.0 para Windows Servers). Também tem de seleccionar o tipo de tarefa. As tarefas possíveis para o Kaspersky Anti-Virus 6.0 são:

- *Verificação de vírus* – verifica a existência de vírus nas áreas especificadas pelo utilizador
- *Actualização* – recolhe e aplica pacotes de actualização para o programa
- *Reversão de Actualização* – reverte a última actualização do programa que foi efectuada
- *Instalação de Chave de Licença* – adicionar uma nova chave de licença para utilizar a aplicação

Passo 3. Configurar definições para o tipo de tarefa seleccionado

Dependendo do tipo de tarefa seleccionado no passo anterior, os conteúdos das janelas que se seguem podem variar:

VERIFICAÇÃO DE VÍRUS

A janela de configuração da tarefa de verificação de vírus requer que você crie uma lista de objectos a verificar (ver 8.2 na pág. 88) e que especifique a acção que o Kaspersky Anti-Virus irá tomar, quando detectar um objecto perigoso (ver 8.4.4 na pág. 97).

ACTUALIZAÇÃO

Para as tarefas de actualização das assinaturas de ameaças e dos módulos da aplicação, tem de especificar a origem que será utilizada para transferir as actualizações (ver 10.4.1 na pág. 111). Por defeito, a origem de actualização é o servidor de actualização do Kaspersky Administration Kit.

REVERSÃO DE ACTUALIZAÇÃO

Não existem definições específicas para reverter a actualização mais recente.

INSTALAR CHAVE DE LICENÇA

Para as tarefas de instalação de chaves de licença, especifique o caminho para o ficheiro da chave com o botão **Procurar**. Para tornar uma chave adicionada

numa reserva, assinale a opção **Adicionar como chave de reserva**. A chave de reserva tornar-se-á activa quando a actual chave de licença expirar.

O campo por baixo apresenta informação sobre a licença adicionada (número de licença, tipo e a data de validade).

Passo 4. Configurar o início da tarefa com uma conta de utilizador diferente

Neste passo, é-lhe pedido que configure as tarefas para se iniciarem com uma conta de utilizador com privilégios suficientes para aceder ao objecto a ser verificado ou à origem de actualização (ver 6.4 na pág. 67).

Passo 5. Configurar um agendamento

Após configurar as definições da tarefa, ser-lhe-á pedido que configure um agendamento automático da tarefa.

Para o fazer, seleccione a frequência para a execução da tarefa a partir do menu suspenso e ajuste as definições de agendamento na parte inferior da janela.

Passo 6. Concluir a criação de uma tarefa

A última janela do assistente irá informá-lo de que criou uma tarefa com sucesso.

12.2.2.2. Criar tarefas de grupo

Para criar uma tarefa de grupo, siga os seguintes passos:

1. Seleccione o grupo para o qual pretende criar uma tarefa, a partir da árvore da consola.
2. Seleccione a respectiva pasta **Tarefas de Grupo**, abra o menu de contexto e seleccione o comando **Criar→Tarefa** ou use o mesmo comando no menu **Acções**. O assistente de criação da tarefa irá então iniciar-se, da mesma forma que o assistente para criar uma tarefa local (para mais informações, ver 12.2.2.1 na pág. 161). Siga as suas instruções.

Quando o assistente estiver concluído, a tarefa será adicionada à pasta **Tarefas de Grupo** daquele grupo e de todos os grupos por baixo do mesmo e estará visível na janela de resultados.

12.2.2.3. Criar tarefas globais

Para criar uma tarefa global, siga os seguintes passos:

1. Seleccione o nódulo **Tarefas globais** na árvore da consola, abra o menu de contexto e seleccione o comando **Criar→Tarefa** ou use o mesmo comando no menu **Acções**.
2. O assistente de criação da tarefa irá então iniciar-se, da mesma forma que o assistente para criar uma tarefa local (para mais informação, ver 12.2.2.1 na pág. 161). A excepção é que existe uma etapa para criar uma lista de computadores cliente a partir da rede, para os quais a tarefa global está a ser criada.
3. Seleccione na rede os computadores que irão executar a tarefa. Pode seleccionar computadores de pastas múltiplas ou seleccionar uma pasta inteira (para mais detalhes, veja o Guia do Administrador para o Kaspersky Administration Kit 6.0).

As tarefas globais apenas são efectuadas num conjunto seleccionado de computadores. Se forem adicionados novos computadores cliente a um grupo com computadores para os quais foi criada uma tarefa de instalação remota, esta tarefa não será executada para esses novos computadores. Tem de criar uma nova tarefa ou fazer as alterações correspondentes nas definições da tarefa existente.

Quando o assistente estiver concluído, será adicionada uma tarefa global ao nódulo **Tarefas globais** da árvore da consola e estará visível na janela de resultados.

12.2.3. Configurar definições de tarefas

Para ver e alterar as definições de tarefas do computador cliente:

1. Abra a janela de propriedades para o computador cliente no separador **Tarefas** (ver Figura 58).
2. Seleccione a tarefa na lista e clique no botão **Propriedades**. Como resultado, abrir-se-á uma janela de definições da tarefa (ver Figura 60).

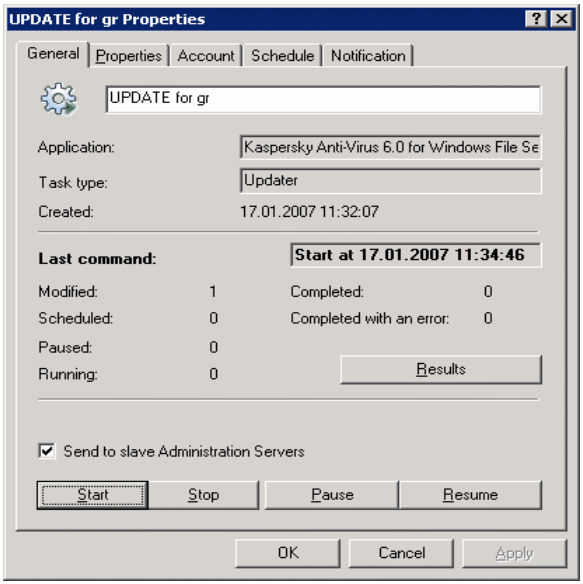


Figura 59. Configurar definições de tarefa

Todos os separadores, com excepção do separador **Definições,** são separadores padrão para o Kaspersky Administration Kit 6.0. Estes são abordados em maior detalhe no Manual de Utilização do Administrador. O separador **Definições** contém definições específicas para o Kaspersky Anti-Virus. Os conteúdos deste separador variam, dependendo do tipo de tarefa seleccionada.

A configuração das definições de tarefa do programa através da interface do Kaspersky Administration Kit é semelhante à configuração através da interface local do Kaspersky Anti-Virus, com a excepção das definições que são específicas daquela tarefa. Veja o Capítulo 7 – Capítulo 10 na pp. 73 – 107 deste Manual do Utilizador para uma descrição mais aprofundada da configuração de definições de tarefa.

Se tiver sido criada uma política para a aplicação (ver 12.3 na pág. 165) que impede que algumas definições sejam reconfiguradas, estas não serão editáveis ao configurar as tarefas.

12.3. Gerir políticas

A configuração de políticas permite-lhe aplicar definições universais da aplicação e das tarefas aos computadores cliente que pertencem a um único grupo da rede.

Esta secção inclui informação sobre a criação e configuração de políticas do Kaspersky Anti-Virus 6.0 para Windows Servers. Para mais informação sobre o conceito de gestão de políticas através do Kaspersky Administration Kit 6.0, veja o Guia do Administrador para o programa.

12.3.1. Criar políticas

Para criar uma política para o Kaspersky Anti-Virus, siga os seguintes passos:

1. Seleccione o grupo de computadores para os quais precisa de criar uma política (ver Figura 54) na pasta **Grupos**.
2. Seleccione a pasta **Políticas** que pertence ao grupo seleccionado, abra o menu de contexto e use o comando **Criar→Política**. Aparecerá uma janela Criar Nova Política.

   A janela Criar Nova Política é concebida como um Assistente padrão do Microsoft Windows e consiste numa série de passos e você pode navegar entre eles utilizando os botões **Anterior** e **Seguinte** ou finalizar com o botão **Concluir**. O botão **Cancelar** irá parar o Assistente em qualquer ponto.

Durante cada passo da criação de uma política, as definições inseridas podem ser bloqueadas com o botão . Se o cadeado do botão estiver fechado, no futuro os valores atribuídos pela política criada serão utilizados quando usar a política nos computadores cliente.

Passo 1. Introduzir dados gerais na política

As primeiras janelas assistente são introdutórias. Aqui deve especificar o nome da política (o campo **Nome**), seleccionar o **Kaspersky Anti-Virus 6.0 para Windows Servers** a partir do menu suspenso **Nome da aplicação**. Se quiser que as definições de política entrem imediatamente em efeito depois de a ter criado, assinale a opção **Tornar a política activa**.

Passo 2. Seleccionar o estado de uma política

Esta janela pedir-lhe-á para especificar o estado da política. Para o fazer, desloque o indicador para a posição desejada: política active ou política inactiva.

Podem ser criadas várias políticas num grupo para uma aplicação, mas apenas uma delas pode ser a política actual (activa).

Passo 3. Seleccionar e configurar as componentes de protecção

Nesta etapa, você pode activar/desactivar a protecção do computador e o Anti-Vírus de Ficheiros. Por defeito, a protecção está activada e o Anti-Vírus de Ficheiros está a funcionar.

Para ajustar as definições de protecção ou para configurar o Anti-Vírus de Ficheiros, seleccione-os na lista e clique no botão **Definições**.

Passo 4. Configurar tarefas de verificação de vírus

Nesta etapa, é-lhe pedido para configurar as definições que serão usadas para tarefas de verificação de vírus.

Na caixa **Nível de segurança**, seleccione um dos três níveis de segurança pré-configurados (ver 7.1 na pág. 74). Para ajustar o nível seleccionado, clique no botão **Definições**. Para restaurar as definições do nível de protecção **Recomendado**, use o botão **Predefinições**.

Na secção **Acções**, especifique a acção que o Anti-Vírus deve tomar quando for detectado um objecto perigoso (ver 8.4.4 na pág. 97).

Passo 5. Configurar definições de actualização

Nesta janela, configure as definições para a função de distribuição de actualizações do Kaspersky Anti-Virus.

Na secção **Definições de actualização**, especifique se os módulos do programa precisam de ser actualizados (ver 10.4.2 na pág. 111). Na janela que se abre quando clica no botão **Definições**, atribua as definições locais de rede (ver 10.4.3 na pág. 116) e especifique a origem de actualização (ver 10.4.1 na pág. 111).

Na secção **Acção após Actualização**, active/desactive a verificação da Quarentena após a recepção de um novo pacote de actualização (ver 10.4.4 na pág. 118).

Passo 6. Implementação da política

Nesta etapa, é-lhe pedido que seleccione um método para distribuir a política pelos clientes do grupo (para mais detalhes, consulte o Guia do Administrador do Kaspersky Administration Kit 6.0).

Passo 7. Determinação de um método para a aplicação inicial da política

Neste passo, seleccione um método para a aplicação inicial da política para os computadores cliente do grupo na janela **Aplicar política** (para mais detalhes, veja o Guia do Administrador do Kaspersky Administration Kit 6.0).

Passo 8. Concluir a criação de uma política

A janela final do assistente informa-o de que criou uma política com sucesso.

Assim que o assistente estiver concluído, a política do Kaspersky Anti-Virus será adicionada à pasta **Políticas** para o grupo correspondente e estará visível na janela de resultados.

Pode editar as definições da política criada e definir restrições à alteração das suas definições, utilizando o botão para cada grupo de definições. Se essas definições estiverem bloqueadas, um utilizador no computador cliente não poderá alterar as definições. A política será aplicada aos computadores cliente na primeira vez que os clientes sincronizarem com o servidor.

Pode copiar ou mover políticas de um grupo para outro e apagá-las, utilizando os comandos padrão **Copiar/Colar**, **Cortar/Colar** e **Apagar** a partir do menu de contexto ou os mesmos comandos a partir do menu **Acções**.

12.3.2. Ver e editar definições da política

Na etapa de edição, pode alterar a política e bloquear a alteração das definições em políticas de grupos aninhados e em definições da aplicação e de tarefas.

Para ver e editar as definições de políticas:

1. Seleccione o grupo de computadores para o qual precisa de editar as definições, a partir da árvore da consola na pasta **Grupos**.
2. Seleccione uma pasta **Políticas** que pertença àquele grupo. Quando o fizer, a janela de resultados apresentará todas as políticas criadas para o grupo.

3. Seleccione a política de que precisa a partir da lista de políticas do **Kaspersky Anti-Virus 6.0 para Windows Servers** (o nome da aplicação é especificado no campo **Aplicação**).
4. Abra o menu de contexto para a política seleccionada e clique no comando **Propriedades**. O ecrã apresentará a janela de definições da política para o Kaspersky Anti-Virus 6.0 (ver Figura 60).

Todos os separadores, com excepção do separador **Definições,** são separadores padrão para o Kaspersky Administration Kit 6.0. Estes são abordados em maior detalhe no Manual de Utilização do Administrador.

O separador **Definições** apresenta as definições da política para o Kaspersky Anti-Virus 6.0. As definições da política incluem as definições do programa (ver 12.1.2 na pág. 156) e as definições de tarefas (ver 12.2 na pág. 159).

Para configurar as definições, seleccione o valor necessário do menu suspenso na parte superior da janela e configure as definições.

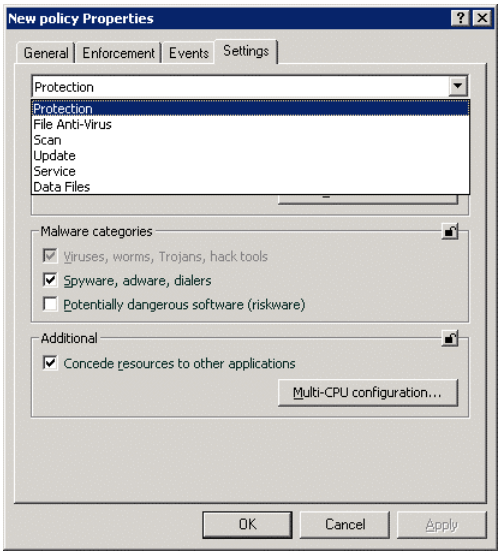


Figura 60. Configurar definições de política

CAPÍTULO 13. TRABALHAR COM O PROGRAMA A PARTIR DA LINHA DE COMANDOS

Você pode utilizar o Kaspersky Anti-Virus para Windows Servers a partir de um comando de acção. Pode executar as seguintes operações:

- Iniciar, parar, pausar e retomar a actividade do Anti-Virus de Ficheiros
- Iniciar, parar, pausar e retomar as verificações de vírus
- Obter informação sobre o estado actual do Anti-Virus de Ficheiros, tarefas e estatísticas sobre os mesmos
- Verificar ficheiros seleccionados
- Actualizar assinaturas de ameaças e módulos do programa
- Aceder à Ajuda para a sintaxe de acção do comando
- Aceder à Ajuda para a sintaxe do comando

A sintaxe na linha de comandos é:

```
avp.com <command> [settings]
```

Tem que aceder ao programa através do comando de acção a partir da pasta de instalação do programa ou especificando o caminho completo para avp.com.

Os seguintes elementos podem ser utilizados como **<commands>**:

ADDKEY	Activa a aplicação utilizando um ficheiro de chave (comando que só pode ser executado se for inserida a password atribuída através da interface do programa)
ACTIVATE	Activa a aplicação através da Internet, utilizando um código de activação
START	Inicia o Anti-Vírus de Ficheiros ou uma tarefa
PAUSE	Pausa o Anti-Vírus de Ficheiros ou uma tarefa (comando que só pode ser executado se for inserida a password atribuída através da interface do programa)

RESUME	Retoma o Anti-Vírus de Ficheiros ou uma tarefa
STOP	Pára o Anti-Vírus de Ficheiros ou uma tarefa (comando que só pode ser executado se for inserida a password atribuída através da interface do programa)
STATUS	Mostra o estado do Anti-Vírus de Ficheiros ou da tarefa actualmente no ecrã
STATISTICS	Mostra as estatísticas para o Anti-Vírus de Ficheiros ou tarefa no ecrã
HELP	Ajuda com a sintaxe do comando e a lista de comandos
SCAN	Analisa objectos em termos de vírus
UPDATE	Inicia a actualização do programa
ROLLBACK	Reverte para a última actualização do programa (comando que só pode ser executado se for inserida a password atribuída através da interface do programa)
EXIT	Fecha o programa (você só poderá executar este comando com a password atribuída na interface do programa)
IMPORT	Importa as definições de protecção do Kaspersky Anti-Virus para Windows Servers (comando que só pode ser executado se for inserida a password atribuída através da interface do programa)
EXPORT	Exporta as definições de protecção do Kaspersky Anti-Virus para Windows Servers

Cada comando usa as suas próprias definições específicas para aquela componente do Kaspersky Anti-Virus para Windows Servers.

13.1. Activar a aplicação

Pode activar o programa de duas formas:

- Online, utilizando um código de activação (o comando ACTIVATE)

- Utilizando um ficheiro de chave de licença (o comando ADDKEY).

Sintaxe do comando:

```
ACTIVATE <activation_code>
ADDKEY <file_name> /password=<your_password>
```

Parâmetros:

<file_name>	Nome do ficheiro de chave de licença com a extensão *.key.
<activation_code>	Código de activação do programa fornecido quando o adquiriu.
<your_password>	Password para aceder ao Kaspersky Anti-Virus, atribuída na interface da aplicação.
Note que este comando não será aceite sem uma password.	

Exemplo:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<your_password>
```

13.2. Gerir o Anti-Vírus de Ficheiros e tarefas

Sintaxe do comando:

```
avp.com <command> <profile|task_name>
[/R[A]:<log_file>]
avp.com STOP|PAUSE <profile|task_name>
/password=<your_password> [/R[A]:<report_file>]
```

Parâmetros:

<command>	Você pode gerir as componentes e tarefas do Kaspersky Anti-Virus a partir do comando de acção com estes comandos: **START** – iniciar uma componente de protecção em tempo real ou tarefa. **STOP** – parar uma componente de protecção em

	tempo real ou tarefa. **PAUSE** – pausar uma componente de protecção em tempo real ou tarefa. **RESUME** – retomar uma componente de protecção em tempo real ou tarefa. **STATUS** – apresentar o actual estado da componente de protecção em tempo real ou tarefa. **STATISTICS** – apresenta estatísticas no ecrã sobre o funcionamento da componente de protecção em tempo real ou tarefa. Note que os comandos PAUSE e STOP estão protegidos por password.
<profile|task_name>	O parâmetro **<profile>** pode ser atribuído a qualquer componente de protecção em tempo real, módulos das componentes, tarefas de verificação a pedido ou actualizações como valor (os valores padrão utilizados no programa são apresentados na tabela abaixo apresentada). Os valores válidos para o parâmetro **<task_name>** podem incluir o nome de qualquer tarefa de verificação ou actualização a pedido definida pelo utilizador.
<your_password>	A password do Kaspersky Anti-Virus atribuída na interface do programa.
/R[A]:<report_file>	**R:<report_file>**: apenas regista eventos importantes no relatório. **/RA:<report_file>**: regista todos os eventos no relatório. Pode utilizar um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, os resultados da verificação são exibidos no ecrã e todos os eventos são apresentados.

Um dos seguintes valores é atribuído a **<profile>**:

RTP	Todas as componentes de protecção O comando `avp.com START RTP` inicia o Anti-Vírus de Ficheiros, se este tiver sido pausado através do botão na interface gráfica do utilizador ou através do comando **PAUSE** na linha de comandos. Se a componente foi desactivada através do botão na interface gráfica do utilizador ou através do comando **STOP** na linha de comandos, tem que executar o comando `avp.com START FM` para o iniciar.
FM	Anti-Vírus de Ficheiros
UPDATER	Actualizador
RetranslationCfg	Distribuição de actualizações numa origem de actualização local
Rollback	Reverte para a última actualização do programa
SCAN_OBJECTS	Tarefa de verificação de vírus
SCAN_MY_COMPUTER	Tarefa O Meu Computador
SCAN_CRITICAL_AREAS	Tarefa Áreas Críticas
SCAN_STARTUP	Tarefa Objectos de Inicialização
SCAN_QUARANTINE	Tarefa para verificação de objectos da quarentena
As componentes e tarefas iniciadas a partir do comando de acção trabalham com as definições configuradas na interface do programa.	

Exemplos:

Para activar o Anti-Vírus de Ficheiros, digite isto na linha de comandos:

```
avp.com START FM
```

Para parar uma tarefa de verificação “O Meu Computador” a partir da linha de comandos, introduza*:*

```
avp.com STOP SCAN_MY_COMPUTER
/password=<your_password>
```

13.3. Verificação Anti-Virus

A sintaxe para iniciar uma verificação de vírus de determinada área e processar ficheiros maliciosos a partir de um comando de acção tem, geralmente, o seguinte aspecto:

```
avp.com SCAN [<object scanned>] [<action>] [<file
types>] [<exclusions>] [<configuration file>]
[<report settings>] [<advanced settings>]
```

Para analisar ficheiros, você também pode utilizar as tarefas criadas no Kaspersky Anti-Virus para Windows Servers, iniciando a tarefa que necessita a partir da linha de comandos (ver 13.2 na pág. 172). A tarefa será executada com as definições especificadas na interface do programa.

Descrição de parâmetro:

<object scanned> - este parâmetro dá-lhe a lista de ficheiros que serão analisados em termos de código malicioso. Pode incluir vários valores da lista fornecida, separados por espaços.	
<files>	Lista de caminhos para os ficheiros e/ou pastas a serem analisados. Pode introduzir caminhos absolutos ou relativos. Os itens da lista estão separados por um espaço. Notas: Se o nome do ficheiro tiver um espaço, deve ser colocado entre aspas Se seleccionar uma pasta específica, todos os ficheiros existentes na mesma serão analisados.
/MEMORY	Objectos da memória do sistema
/STARTUP	Objectos de inicialização
/MAIL	Bases de dados de e-mails

/REMDRIVES	Todos os discos removíveis
/FIXDRIVES	Todos os discos rígidos
/NETDRIVES	Todos os discos de rede
/QUARANTINE	Objectos em quarentena
/ALL	Verificação completa
/@:<filelist.lst>	Caminho para um ficheiro com uma lista de objectos e pastas a serem incluídos na verificação. O ficheiro deve estar em formato texto e cada objecto de verificação deve iniciar uma linha nova. Pode introduzir um caminho absoluto ou relativo para o objecto. O caminho deve ser colocado entre aspas se tiver um espaço.
`<action>` - este parâmetro define respostas aos objectos maliciosos detectados durante a verificação. Se este parâmetro não for definido, o valor predefinido é **`/i8`**.	
`/i0`	Não actua sobre o objecto; simplesmente guarda informação sobre o mesmo no relatório.
`/i1`	Trata objectos infectados e, se a desinfecção falhar, ignora-os.
`/i2`	Trata objectos infectados e, se a desinfecção falhar, apaga-os. Excepções: não apaga objectos infectados de objectos compostos e apaga objectos compostos com cabeçalhos executáveis (arquivos sfx) (esta é a predefinição).
`/i3`	Trata objectos infectados e, se a desinfecção falhar, apaga-os. Para além disso, apaga completamente todos os objectos compostos se os conteúdos infectados não puderem ser apagados.

/i4	Apaga objectos infectados e, se a desinfecção falhar, apaga-os. Para além disso, apaga completamente todos os objectos compostos se os conteúdos infectados não puderem ser apagados.
/i8	Solicitar a acção a efectuar se for detectado um objecto infectado
/i9	Solicitar a acção a efectuar no final da verificação
<file types> - este parâmetro define os tipos de ficheiros que serão sujeitos à verificação do Anti-Vírus. Se este parâmetro não estiver definido, o valor por defeito é /fi.	
/fe	Verifica por extensão só os ficheiros potencialmente infectados
/fi	Verifica por conteúdo só os ficheiros potencialmente infectados
/fa	Verifica todos os ficheiros
<exclusions> - este parâmetro define os objectos excluídos da verificação. Pode incluir vários valores a partir da lista fornecida, separados por espaços.	
-e:a	Não verifica arquivos
-e:b	Não verifica bases de dados de e-mails
-e: m	Não verifica e-mail com texto simples
-e:<filemask>	Não verifica ficheiros por máscara
-e:<seconds>	Ignora os ficheiros que são verificados durante um tempo superior àquele especificado no parâmetro <**seconds**> (segundos).
-es:<size>	Ignora ficheiros com tamanho superior (em MB) ao valor atribuído por **<tamanho>**.

<configuration file> - define o caminho para o ficheiro de configuração que contém as definições do programa para a verificação. O ficheiro de configuração é guardado em formato binário (*.dat*), a não ser que tenha sido especificado outro formato ou se o formato não estiver atribuído e pode ser usado mais tarde para importar definições da aplicação para outros computadores. Pode introduzir um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, são utilizados os valores definidos na interface do Kaspersky Anti-Virus para Windows Servers.	
/C:<file_name>	Utiliza os valores das definições atribuídas no ficheiro de configuração **<file_name>**
<report settings> - este parâmetro determina o formato do relatório dos resultados da verificação. Pode usar um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, os resultados da verificação são exibidos no ecrã e todos os eventos são apresentados.	
/R:<report_file>	Só regista eventos importantes neste ficheiro
/RA:<report_file>	Regista todos os eventos neste ficheiro
<advanced settings> – definições que determinam a utilização das tecnologias de verificação Anti-Vírus.	
/iChecker=<on|off>	Activar/ desactivar iChecker.
/iSwift=<on|off>	Activar/ desactivar iSwift.

Exemplos:

*Iniciar uma verificação da RAM, Programas de Inicialização, bases de dados do e-mails, os directórios **Os Meus Documentos** e **Ficheiros de Programa** e o ficheiro **test.exe**:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Pausar a verificação dos objectos seleccionados e iniciar a verificação completa do computador e depois continuar a verificação de vírus dentro dos objectos seleccionados:

```
avp.com PAUSE SCAN_OBJECTS /password=<your_password>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*Verificar os objectos listados no ficheiro **object2scan.txt**. Utilizar o ficheiro de configuração **scan_setting.txt** para a tarefa. Depois da verificação, gerar um relatório em que são guardados todos os eventos:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

Uma amostra de um ficheiro de configuração:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

13.4. Actualizações do programa

A sintaxe para actualizar os módulos do programa e as assinaturas de ameaças do Kaspersky Anti-Virus para Windows Servers a partir do comando de acção é a seguinte:

```
avp.com UPDATE [<update_source>] [/R[A]:<report_file>]
[/C:<file_name>] [/APP=<on|off>]
```

Descrição do parâmetro:

<update_source>	Servidor HTTT ou FTP ou directório de rede para transferir actualizações. Pode especificar o caminho absoluto para a origem de actualização ou um URL como o valor deste parâmetro. Se não for especificado nenhum caminho, a origem de actualização será copiada das definições de actualização.

/R[A]:<report_file>	**/R:<report_file>** – só regista eventos importantes no relatório. **/R[A]:<report_file>** – regista todos os eventos no relatório. Pode introduzir um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, os resultados da verificação são exibidos no ecrã e todos os eventos são apresentados.
/C:<file_name>	Caminho para o ficheiro de configuração com as definições das actualizações do programa. O ficheiro de configuração é um ficheiro de texto que contém um conjunto de definições da linha de comandos para a actualização do programa. Pode introduzir um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, são utilizados os valores das definições configuradas na interface do Kaspersky Anti-Virus para Windows Servers.
/APP=<on|off>	Activar / Desactivar actualizações dos módulos da aplicação

Exemplos:

Actualizar assinaturas de ameaças e gravar todos os eventos no relatório:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Actualizar os módulos do programa Kaspersky Anti-Virus para Windows Servers utilizando as definições no ficheiro de configuração **updateapp.ini**:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Uma amostra de um ficheiro de configuração:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app=on
```

13.5. Definições de reversão

Sintaxe do comando:

```
ROLLBACK
[/R[A]:<report_file>][/password=<your_password>]
```

/R[A]:<report_file>	**/R:<report_file>** – só regista eventos importantes no relatório. **/R[A]:<report_file>** – regista todos os eventos no relatório. Pode introduzir um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, os resultados da verificação são exibidos no ecrã e todos os eventos são apresentados.
<your_password>	Password para aceder ao Kaspersky Anti-Virus, atribuída na interface da aplicação.
Note que não pode executar este comando sem inserir a password.	

Exemplo:

```
avp.com ROLLBACK /RA:rollback.txt
[/password=<password>]
```

13.6. Exportar definições

Sintaxe do comando:

```
avp.com EXPORT <profile> <file_name>
```

Descrição do parâmetro:

<profile>	Anti-Vírus de Ficheiros ou tarefa com as definições a ser exportadas. Pode utilizar qualquer valor para **<profile>** que está listado na secção 13.2 na pág. 172.

<file_name>	Caminho para o ficheiro para o qual são exportadas as definições do Kaspersky Anti-Virus para Windows Servers. Pode utilizar um caminho absoluto ou relativo. O ficheiro de configuração é guardado em formato binário (*.dat*), a não ser que tenha sido especificado outro formato ou se o formato não estiver atribuído e pode ser usado mais tarde para importar definições da aplicação para outros computadores. O ficheiro de configuração pode ser guardado como um ficheiro de texto. Para o fazer, especifique a extensão *.txt* no nome do ficheiro. Note que não pode importar as definições de protecção a partir de um ficheiro de texto. Este ficheiro apenas pode ser usado para especificar as principais definições do funcionamento do programa.

Exemplos:

```
avp.com EXPORT c:\settings.dat
```

13.7. Importar definições

Sintaxe do comando:

```
avp.com IMPORT <file_name>
[/password=<your_password>]
```

<file_name>	Caminho para o ficheiro a partir do qual são importadas as definições do Kaspersky Anti-Virus para Windows Servers. Pode utilizar um caminho absoluto ou relativo. As definições só podem ser importadas a partir de ficheiros binários. Se instalar o programa em modo oculto a partir da linha de comandos ou com o Editor de Objectos de Política de Grupo, então o nome do ficheiro de configuração deve ser *install.cfg*. Caso contrário, o programa não irá reconhecê-lo.
<your_password>	Password para o Kaspersky Anti-Virus atribuída na interface da aplicação.

Note que este comando não será aceite sem uma password.

Exemplo:

```
avp.com IMPORT c:\settings.dat /password=<your_password>
```

13.8. Iniciar o programa

Sintaxe do comando:

```
avp.com
```

13.9. Parar o programa

Sintaxe do comando:

```
EXIT /password=<password>
```

<password>	A password do Kaspersky Anti-Virus atribuída na interface do programa.
Note que este comando não será aceite sem uma password.	

Note que não pode executar este comando sem introduzir uma password.

13.10. Obter um Ficheiro de Rastreio

Você pode precisar de criar um ficheiro de rastreio se tiver problemas com a execução da aplicação para resolvê-los com maior exactidão com os especialistas do Suporte Técnico.

Sintaxe do comando:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

[on|off]	Activar/desactivar criação de ficheiro de rastreio.
[file]	Obter um rastreio e guardar num ficheiro.

<trace_level>	Este parâmetro pode ter atribuídos valores numéricos de 0 (nível mínimo, apenas eventos críticos) a 700 (nível máximo, todos os eventos). Um especialista dir-lhe-á que nível de rastreio necessita quando contactar o Suporte. Se isso não for especificado, recomendamos que configure o nível para 500.
Aviso: Apenas recomendamos a criação de ficheiros de rastreio para a resolução de um problema específico. A activação regular dos ficheiros de rastreio pode tornar o seu computador mais lento e encher o seu disco rígido.	

Exemplos:

Para desactivar rastreio:

```
avp.com TRACE file off
```

Para criar um ficheiro de rastreio para enviar ao Suporte Técnico com um nível de rastreio máximo de 500:

avp.com TRACE file on 500

13.11. Visualizar o Menu Ajuda

Este comando está disponível para visualizar o Menu Ajuda sobre a sintaxe do comando de acção:

```
avp.com [ /? | HELP ]
```

Para pedir ajuda sobre a sintaxe de um comando específico, pode utilizar um dos seguintes comandos:

```
avp.com <command> /?
avp.com HELP <command>
```

13.12. Códigos de retorno da interface da linha de comandos

Esta secção contém uma lista dos códigos de retorno da linha de comandos. Os códigos gerais podem ser devolvidos por qualquer comando da linha de comandos. Os códigos de retorno incluem códigos gerais, assim como códigos específicos de um tipo de tarefa específico.

Códigos de retorno gerais	
0	Operação concluída com sucesso
1	Valor de definição inválido
2	Erro desconhecido
3	Erro de conclusão da tarefa
4	Tarefa cancelada
Códigos de retorno das tarefas de verificação do Anti-Virus	
101	Todos os objectos perigosos foram processados
102	Objectos perigosos detectados

CAPÍTULO 14. MODIFICAR, REPARAR E REMOVER O PROGRAMA

Pode desinstalar a aplicação das seguintes formas:

- Usando o Assistente de Instalação da aplicação (ver 14.2 na pág. 189);
- A partir da linha de comandos (ver 14.2 na pág. 189);
- Usando o Kaspersky Administration Kit (ver Guia de Implementação do Kaspersky Administration Kit);
- Usando as políticas de domínios de grupos do Microsoft Windows Server 2000/2003 (ver 3.4.3 na pág. 36).

14.1. Modificar, reparar e remover o programa com o Assistente de Instalação

Você poderá precisar de reparar o programa se detectar erros no seu funcionamento depois de uma configuração incorrecta ou corrupção de um ficheiro.

Para reparar ou modificar as componentes em falta do Kaspersky Anti-Virus para Windows Servers ou apagar o programa:

1. Introduza o CD de instalação na unidade de CD-ROM, se utilizou um CD para instalar o programa. Se instalou o Kaspersky Anti-Virus para Windows Servers a partir de uma origem diferente (pasta de acesso público, pasta no disco rígido, etc.), certifique-se de que o pacote de instalação está na origem especificada e que você pode aceder ao mesmo.
2. Seleccione **Iniciar → Programas → Kaspersky Anti-Virus 6.0 para Windows Servers → Modificar, Reparar ou Remover**.

Um assistente de instalação abrir-se-á. Vejamos, mais detalhadamente, os passos para reparar, modificar ou apagar o programa.

Passo 1. Janela de Boas-vindas da instalação

Se seguir todos os passos acima mencionados, necessários para reparar ou modificar o programa, aparecerá a janela de boas-vindas da instalação do Kaspersky Anti-Virus para Windows Servers. Para continuar, clique no botão **Seguinte**.

Passo 2. Seleccionar uma operação

Neste passo, selecciona a operação que deseja executar. Pode modificar as componentes do programa, reparar as componentes existentes ou remover componentes ou o programa todo. Para efectuar a operação de que necessita, clique no botão apropriado. A resposta do programa depende da operação que seleccionar.

Modificar o programa é semelhante a personalizar a instalação do programa, onde pode especificar que componentes deseja instalar (ver Passo 7 na pág. 26) e quais deseja apagar.

A reparação do programa depende das componentes do programa instaladas. Os ficheiros serão reparados para todas as componentes instaladas e o nível de segurança Recomendado será configurado para cada uma delas.

Aviso!

Se o Kaspersky Anti-Virus 6.0 for desinstalado de forma remota, o servidor não se reiniciará automaticamente. Contudo, para remover por completo as componentes da aplicação e para que o computador funcione de forma correcta no futuro, recomendamos que reinicie o servidor manualmente.

Se remover o programa, pode seleccionar que dados criados e utilizados pelo programa deseja guardar no seu computador. Para apagar todos os dados do Kaspersky Anti-Virus para Windows Servers, seleccione **Concluir desinstalação**. Para guardar dados, seleccionar **Guardar os objectos da aplicação** e especifique que objectos não deseja apagar:

- *Dados de activação* – informação sobre a activação do programa.
- *Assinaturas de ameaças* – conjunto completo das assinaturas de programas perigosos, vírus e outras ameaças actuais desde a última actualização.
- *Ficheiros de Cópia de Segurança* – cópias de segurança de ficheiros apagados ou desinfectados. Recomenda-se que sejam guardados, caso possam ser restaurados mais tarde.
- *Ficheiros de Quarentena* – ficheiros que estão potencialmente infectados por vírus ou modificações de vírus. Estes ficheiros contêm código similar

ao código de um vírus conhecido, mas é difícil determinar se são maliciosos. Recomenda-se que sejam guardados, uma vez que, na verdade, podem não estar infectados ou podem ser desinfectados depois da actualização das assinaturas de ameaças.

- *Definições da aplicação* – configurações para o Anti-Vírus de Ficheiros.
- *Dados do iSwift* – base de dados com informação sobre objectos verificados em sistemas de ficheiros NTFS, o que pode aumentar a velocidade de verificação. Quando utiliza esta base de dados, o Kaspersky Anti-Virus para Windows Servers só analisa os ficheiros que foram modificados desde a ultima verificação.

Aviso!

Se passar um longo período de tempo entre a desinstalação de uma versão do Kaspersky Anti-Virus para Windows Servers e a instalação de uma outra versão, não recomendamos a utilização da base de dados do *iSwift* de uma instalação anterior. Um programa perigoso poderá penetrar no computador durante este período e os seus efeitos não seriam detectados pela base de dados, o que poderia levar a uma infecção.

Para iniciar a operação seleccionada, clique no botão **Seguinte**. O programa começará a copiar os ficheiros necessários para o seu computador ou a apagar as componentes e dados seleccionados.

Passo 3. Concluir a modificação, reparação ou remoção do programa

O processo de modificação, reparação ou remoção será mostrado no ecrã, após o qual você será informado da sua conclusão.

Normalmente, a remoção do programa implica que reinicie o seu computador, já que isso é necessário para assumir as modificações ao seu sistema. O programa pedir-lhe-á para reiniciar o seu computador. Clique em **Sim** para reiniciar imediatamente. Para reiniciar o seu computador mais tarde, clique em **Não**.

14.2. Desinstalar o programa a partir da linha de comandos

Para desinstalar o Kaspersky Anti-Virus 6.0 para Windows Servers a partir da linha de comandos, introduza:

```
msiexec /x <package_name>
```

O Assistente de Instalação abrir-se-á. Pode usá-lo para desinstalar a aplicação (ver Capítulo 14 na pág. 186).

Para desinstalar a aplicação de forma não interactiva sem reiniciar o computador (o computador deverá ser manualmente reiniciado depois da instalação), digite:

```
msiexec /x <package_name> /qn
```

Para desinstalar a aplicação em segundo plano e depois reiniciar o computador, digite:

```
msiexec /x <package_name> ALLOWREBOOT=1 /qn
```

Se, ao instalar o programa, optou por proteger com password a desinstalação do programa, é necessário introduzir esta password. Caso contrário, o programa não poderá ser desinstalado.

Para remover a aplicação, introduzindo uma password como prova do privilégio de remoção, digite:

`msiexec /x <package_name> KLUNINSTPASSWD=******` – para remover a aplicação no modo interactivo;

`msiexec /x <package_name> KLUNINSTPASSWD=****** /qn` – para remover a aplicação no modo não interactivo;

APÊNDICE A. INFORMAÇÃO DE REFERÊNCIA

Este apêndice contém materiais de referência sobre os formatos de ficheiro e as máscaras de extensão utilizadas pelas definições do Kaspersky Anti-Virus para Windows Servers.

A.1. Lista de ficheiros verificados por extensão

Se seleccionou a opção **Programas e documentos (por extensão)**, o Anti-Vírus de Ficheiros analisará em detalhe os ficheiros com as extensões abaixo mencionadas.

com – ficheiro executável para um programa

exe – ficheiro executável ou arquivo auto-extraível

sys – controlador do sistema

prg – texto de programa para o dBase, Clipper ou Microsoft Visual FoxPro ou um programa para criação de ficheiros .wav

bin - ficheiro binário

bat - ficheiro batch

cmd - ficheiro de comandos para o Microsoft Windows NT (semelhante a um ficheiro .bat para o DOS), OS/2.

dpl - biblioteca compactada do Borland Delphi

dll - biblioteca de ligação dinâmica

scr - ecrã de entrada do Microsoft Windows

cpl - módulo do painel de controlo do Microsoft Windows

ocx - objecto OLE (Ligação e Incorporação de Objectos) da Microsoft

tsp - programa executado em modo de tempos fraccionados

drv - controlador de dispositivo

vxd - controlador de dispositivo virtual do Microsoft Windows

pif - ficheiro de informações de programa

lnk - ficheiro de ligação do Microsoft Windows

reg - ficheiro de chave de registo do sistema do Microsoft Windows

ini - ficheiro de inicialização

cla - classe de Java

vbs - script de Visual Basic

vbe - extensão da BIOS de vídeo

js, jse - texto fonte de JavaScript

htm - documento de hipertexto

htt - cabeçalho de hipertexto do Microsoft Windows

hta - programa de hipertexto para o Microsoft Internet Explorer

asp - script de Active Server Pages (Páginas de Servidor Activas)

chm - ficheiro HTML compilado

pht - HTML com scripts PHP incorporados

php - script incorporado em ficheiros HTML

wsh - ficheiro do script anfitrião do Microsoft Windows

wsf - script do Microsoft Windows

the - plano de fundo da área de trabalho do Microsoft Windows 95

hlp - ficheiro de ajuda do Windows

eml - ficheiro de e-mail do Microsoft Outlook Express

nws - ficheiro de e-mail novo do Microsoft Outlook Express

msg - ficheiro de e-mail do Microsoft Mail

plg - e-mail

mbx - extensão para os e-mails guardados do Microsoft Office Outlook

*doc** – um documento do Microsoft Word, tal como: *doc* – um documento do Microsoft Word, *docx* – um documento do Microsoft Word 2007 com suporte XML, *docm* – um documento do Microsoft Word 2007 com suporte de Macros

*dot** – um modelo de documento do Microsoft Word, tal como: *dot* – um modelo de documento do Microsoft Word, *dotx* – um modelo de documento do Microsoft Word 2007, *dotm* – modelo de documento do Microsoft Word 2007 com suporte de Macros

fpm - programa de base de dados, ficheiro de início para o Microsoft Visual FoxPro

rtf - documento em Formato de Texto Rico

shs - manipulador de objecto de recorte do Shell

dwg - base de dados de desenhos do AutoCAD

msi - pacote de instalação do Microsoft Windows

otm - projecto VBA para o Microsoft Office Outlook

pdf - documento do Adobe Acrobat

swf - ficheiro do Shockwave Flash

jpg, jpeg, png - formato gráfico de imagens comprimidas

emf - formato de metaficheiro avançado. A próxima geração dos metaficheiros do SO Microsoft Windows. Os ficheiros EMF são suportados pelo Microsoft Windows 16-bit.

ico - ficheiro de ícone

ov? - ficheiros executáveis do MS DOC

*xl** – documentos e ficheiros do Microsoft Office Excel, tais como: *xla* - extensão do Microsoft Office Excel, *xlc* - diagrama, *xlt* - modelos de documento xlsx – uma folha de trabalho do Microsoft Excel 2007, *xltm* – um folha de trabalho do Microsoft Excel 2007 workbook suporte de Macros, *xlsb* – um formato (não-XML) em binário do Microsoft Excel 2007, *xltx* – um modelo do Microsoft Excel 2007, *xlsm* – um modelo do Microsoft Excel 2007 com suporte de Macros, *xlam* – uma extensão do Microsoft Excel 2007 com suporte de Macros.

*pp** – documentos e ficheiros do Microsoft Office PowerPoint, tais como: *pps* - diapositivo do Microsoft Office PowerPoint, *ppt* - apresentação, *pptx* – uma apresentação do Microsoft PowerPoint 2007, *pptm* – uma apresentação do Microsoft PowerPoint 2007 com suporte de Macros, *potx* – um modelo de apresentação do Microsoft PowerPoint 2007, *potm* – um modelo de apresentação do Microsoft PowerPoint 2007 com suporte de Macros, *ppsx* – um apresentação de diapositivos do Microsoft PowerPoint 2007, *ppsm* – uma apresentação de diapositivos do Microsoft PowerPoint 2007 com suporte de Macros, *ppam* – uma extensão do Microsoft PowerPoint 2007 com suporte de Macros.

*md** – documentos e ficheiros do Microsoft Office Access, tais como: *mda* - grupo de trabalho do Microsoft Office Access, *mdb* - base de dados, etc.

sldx – um diapositivo do Microsoft PowerPoint 2007.

sldm – um diapositivo do Microsoft PowerPoint 2007 slcom suporte de Macros.

thmx – um tema do Microsoft Office 2007.

Lembre-se que o verdadeiro formato de um ficheiro pode não corresponder ao formato indicado na extensão do ficheiro.

A.2. Máscaras de exclusão de ficheiros possíveis

Vejamos alguns exemplos de máscaras possíveis que você poderá utilizar ao criar listas de exclusão de ficheiros:

- Máscara sem caminhos de ficheiro:

- ***.exe** – todos os ficheiros com a extensão.exe
- ***.ex?** – todos os ficheiros com a extensão .ex?, onde ? pode representar qualquer caractere único
- **teste** – todos os ficheiros com o nome teste

- Máscaras com caminhos de ficheiro absolutos:
  - **C:\dir*.*** ou **C:\dir*** ou **C:\dir** – todos os ficheiros incluídos na pasta C:\dir\
  - **C:\dir*.exe** – todos os ficheiros com a extensão .exe incluídos na pasta C:\dir\
  - **C:\dir*.ex?** – todos os ficheiros com a extensão .ex? incluídos na pasta C:\dir\, onde ? pode representar qualquer caractere único
  - **C:\dir\teste** – apenas o ficheiro C:\dir\teste
  - Se não pretende que o programa verifique os ficheiros incluídos nas subpastas desta pasta, desmarque a opção ☑ **Incluir subpastas** quando criar a máscara.
- Máscaras com caminhos de ficheiro relativos:
  - **dir*.*** ou **dir*** ou **dir** – todos os ficheiros em todas as pastas **dir**
  - **dir\teste** – todos os ficheiros teste incluídos nas pastas dir\
  - **dir*.exe** – todos os ficheiros com a extensão .exe incluídos em todas as pastas dir\
  - **dir*.ex?** – todos os ficheiros com a extensão .ex? incluídos em todas as pastas C:\dir\ , onde ? pode representar qualquer caractere único

  Se não pretende que o programa verifique os ficheiros incluídos nas subpastas desta pasta, desmarque a opção ☑ **Incluir subpastas** quando criar a máscara.

Dica:

As máscaras de exclusão *.* e * apenas podem ser utilizadas se você atribuir a uma ameaça excluída um veredicto, de acordo com a Enciclopédia de Vírus. Caso contrário, a ameaça especificada não será detectada em nenhum dos objectos. Se utilizar estas máscaras sem seleccionar um veredicto, basicamente isso significa desactivar a monitorização.

Nós também não recomendamos que seleccione uma unidade virtual como uma exclusão que foi criada com base num directório do sistema de ficheiros, utilizando o comando subst. Não há razão para o fazer, uma vez que durante a verificação, o programa considera essa unidade virtual como sendo uma pasta e, por conseguinte, verifica-a.

A.3. Possíveis máscaras de exclusão de ameaças

Quando adicionar, enquanto exclusões, as ameaças com um determinado estado da Enciclopédia de Vírus, você pode especificar:

- O nome completo da ameaça tal como aparece listado na Enciclopédia de Vírus presente em www.viruslist.com (por exemplo, **não é vírus:RiskWare.RemoteAdmin.RA.311 ou Flooder.Win32.Fuxx);**
- o nome da ameaça através da máscara. Por exemplo:
    - **não é vírus* -** exclui da verificação programas legais, mas potencialmente perigosos, assim como programas de brincadeiras (joke programs).
    - ***Riskware.* –** exclui da verificação o riskware (software potencialmente perigoso).
    - ***RemoteAdmin.*** – exclui da verificação todos os programas de administração remota.

A.4. Resumo das definições no ficheiro *setup.ini*

O ficheiro *setup.ini*, localizado na pasta de instalação do Kaspersky Anti-Virus, é utilizado ao instalar o programa no modo não interactivo a partir da linha de

comandos (ver 3.3 na pág. 34) ou utilizando o Editor de Objectos de Política de Grupo (ver 3.4 na pág. 35). O ficheiro contém as seguintes definições:

[Setup] – definições gerais para a instalação do programa.

InstallDir=<caminho para a pasta de instalação do programa>.

Reboot=sim|não – define se o computador deve ou não ser reiniciado depois do programa ser instalado (por defeito, não se reinicia).

SelfProtection=sim|não – define se o Kaspersky Anti-Virus deve ou não activar a Auto-defesa durante a instalação (por defeito, está activada).

MSExclusions=sim|não – define se as exclusões que a Microsoft recomenda para servidores devem ou não ser adicionadas à lista de exclusões do Kaspersky Anti-Virus.

AddPath=sim|não – define se o caminho para avp.com será adicionado à variável de ambiente %Path%.

[Components] – selecciona as componentes a instalar. Se este grupo não contiver nenhum item, serão todas instaladas.

FileMonitor=sim|não – instala o Anti-Vírus de Ficheiros.

[Tasks] – activa as tarefas do Kaspersky Anti-Virus. Se não for especificada nenhuma tarefa, após a instalação todas as tarefas funcionarão. Se tiver especificado algumas tarefas, todas as tarefas que não estiverem listadas serão desactivadas.

ScanMyComputer=sim|não – tarefa para a verificação completa do computador

ScanStartup=sim|não – tarefa para a verificação de objectos de inicialização

ScanCritical=sim|não – tarefa para a verificação de áreas críticas

Updater=sim|não – tarefa para a actualização das assinaturas de ameaças e dos módulos do programa

Em vez do valor **sim**, pode utilizar os valores **1**, **on**, **activar** ou **activado** e em vez de **não** pode usar – **0**, **off**, **desactivar** ou **desactivado**.

APÊNDICE B. KASPERSKY LAB

Fundada em 1997, a Kaspersky Lab tornou-se num líder reconhecido nas tecnologias de segurança de informação. Produz uma ampla gama de software para segurança de dados e fornece soluções de alta performance e abrangentes para proteger computadores e redes em relação a todos os tipos de programas maliciosos, mensagens de e-mail não-solicitadas e indesejadas e ataques de hackers.

A Kaspersky Lab é uma empresa internacional. Centralizada na Federação Russa, a empresa tem filiais representantes no Reino Unido, França, Alemanha, Japão, EUA (Califórnia), Benelux, China, Polónia, e Roménia. Um novo departamento da empresa, o Centro Europeu de Pesquisa Anti-Vírus, foi recentemente criado em França. A rede de parceiros da Kaspersky Lab inclui mais de 500 empresas em todo o mundo.

Hoje, a Kaspersky Lab emprega mais de 450 especialistas, cada um versado em tecnologias Anti-Vírus, em que 10 deles têm graduações M.B.A., 16 têm doutoramentos e especialistas membros da Computer Anti-Virus Researchers Organization (CARO).

A Kaspersky Lab oferece as melhores soluções de segurança, baseadas na sua experiência única e conhecimento, obtidos ao longo de mais de 14 anos a combater vírus de computador. Uma análise detalhada das actividades do vírus de computador permite que a empresa forneça uma protecção global em relação a ameaças correntes e futuras. A resistência a ataques futuros é a política de base implementada em todos os produtos da Kaspersky Lab. Em qualquer altura, os produtos da empresa permanecem um passo à frente de muitos outros vendedores no fornecimento de uma cobertura Anti-Vírus extensiva tanto para utilizadores domésticos, como para empresas.

Anos de árduo trabalho tornaram a empresa num dos melhores fabricantes de software de segurança. A Kaspersky Lab foi uma das primeiras companhias do seu género a desenvolver as melhores normas de defesa Anti-Vírus. O produto emblemático da empresa, o Kaspersky Anti-Virus, permite a protecção total para todos os níveis da rede, incluindo estações, servidores, sistemas de correio electrónico, firewalls, gateways de Internet e computadores portáteis. As suas ferramentas de gestão adequadas e intuitivas asseguram uma automação avançada para a protecção rápida contra vírus em toda a empresa. Muitos fabricantes conhecidos usam o núcleo do Kaspersky Anti-Virus, incluindo a Nokia ICG (EUA), F-Secure (Finlândia), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab beneficiam de uma ampla gama de serviços adicionais que asseguram tanto o funcionamento estável dos produtos da empresa, como a conformidade com as necessidades específicas da empresa.

A base de dados Anti-Vírus da Kaspersky Lab é actualizada a cada hora. A empresa fornece aos seus clientes um serviço de suporte técnico de 24 horas, que está disponível em várias línguas para satisfazer os seus clientes internacionais.

B.1. Outros produtos da Kaspersky Lab

News Agent da Kaspersky Lab

O News Agent (Agente de Notícias) é destinado à entrega, atempada, de notícias publicadas pela Kaspersky Lab, notificações sobre o estado actual da actividade de vírus e notícias recentes. O programa lê a lista de fontes de notícias disponíveis e o seu conteúdo a partir do servidor de notícias da Kaspersky Lab em intervalos especificados.

O News Agent permite aos utilizadores;

- Ver a previsão actual de vírus na bandeja do sistema.
- Subscrever e anular a subscrição de notícias.
- Recolher notícias de cada fonte de notícias seleccionada, no intervalo especificado e receber notificações sobre notícias recentes.
- Rever notícias nas fontes seleccionadas.
- Rever a lista de fontes e o seu estado.
- Abrir textos completos de artigos no seu navegador

O News Agent é uma aplicação independente do Microsoft Windows, que pode ser usada sozinha ou em conjunto com várias soluções integradas oferecidas pela Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

Este programa é um serviço livre fornecido aos visitantes da página de Internet da Kaspersky Lab. O serviço permite uma verificação eficiente e online de vírus no seu computador. O Kaspersky On-Line Scanner Kaspersky OnLine Scanner é executado directamente no navegador da Internet. Assim, os utilizadores recebem respostas rápidas a questões sobre infecções potenciais nos seus computadores. Ao utilizar o serviço, os visitantes podem:

- Excluir da verificação arquivos e bases de dados de e-mail.
- Seleccionar bases de dados padrão/alargadas para a verificação.

- Guardar um relatório sobre os resultados da verificação em formatos txt ou html

Kaspersky® OnLine Scanner Pro

O programa é um serviço de assinatura acessível aos visitantes da página da Web da Kaspersky Lab. O serviço permite uma verificação eficiente e online de vírus no seu computador e desinfecta ficheiros perigosos. O Kaspersky OnLine Scanner Pro é executado directamente no navegador da Internet. Ao utilizar o serviço, os visitantes podem:

- Excluir da verificação arquivos e bases de dados de e-mail.
- Seleccionar bases de dados padrão/alargadas para a verificação.
- Guardar um relatório sobre os resultados da verificação em formatos txt ou html

Kaspersky Anti-Virus® 7.0

O Kaspersky Anti-Virus 7.0 foi concebido para salvaguardar computadores pessoais contra software malicioso, com combinação optimizada de métodos convencionais de protecção Anti-Vírus e de novas tecnologias pró-activas.

O programa permite verificações complexas de vírus, incluindo:

- Verificação Anti-Vírus do tráfego de e-mail ao nível dos protocolos de transmissão de dados (POP3, IMAP e NNTP para mensagens de entrada e SMTP para mensagens de saída), independentemente do cliente e-mail a ser usado, assim como a desinfecção de bases de dados de e-mail.
- Verificação Anti-Vírus, em tempo real, do tráfego de Internet transferido por HTTP.
- Verificação Anti-Vírus em ficheiros individuais, pastas ou unidades. Além disto, pode ser usada uma tarefa predefinida de verificação para iniciar a verificação Anti-Vírus, exclusivamente, para áreas críticas do sistema operativo e objectos de inicialização do Microsoft Windows.

A protecção pró-activa oferece as seguintes funções:

- **Controlo das alterações ao sistema de ficheiros**. O programa permite que os utilizadores criem uma lista de aplicações, que controlará numa base de componentes. Ajuda a proteger a integridade da aplicação face à influência de software malicioso.
- **Monitorização de processos na memória de acesso aleatório**. O Kaspersky Anti-Vírus 7.0 notifica, atempadamente, os utilizadores

quando detecta processos perigosos, suspeitos ou escondidos ou em caso de ocorrerem alterações não-autorizadas em processos activos.

- **Monitorizar alterações no registo do Sistema Operativo** devido ao controlo interno do registo do sistema.
- **Monitorização de Processos Ocultos** ajuda a proteger de código malicioso escondido no sistema operativo através de tecnologias de processos ocultos (rootkit).
- **Analisador Heurístico**. Ao analisar um programa, o analisador simula a sua execução e regista todas as actividades suspeitas, tais como a abertura ou escrita num ficheiro, intercepção de vectores interrompidos, etc. É tomada uma decisão com base neste procedimento relativamente à possível infecção do programa com um vírus. A simulação ocorre num ambiente virtual isolado que protege o computador da infecção.
- **Restauro do sistema** após ataques de software malicioso, registando todas as alterações no registo e no sistema de ficheiros do computador, com a oportunidade para efectuar recuperações a pedido do utilizador.

Kaspersky® Internet Security 7.0

O Kaspersky® Internet Security 7.0 é uma solução integrada para a protecção dos seus computadores pessoais em relação às principais ameaças relacionadas com a informação, ou seja vírus, hackers, spam e spyware. Uma interface de utilizador comum permite a configuração e gestão de todas as componentes da solução.

A função de protecção Anti-Vírus inclui:

- **Análise Anti-Vírus do tráfego de e-mail** ao nível dos protocolos de transmissão de dados (POP3, IMAP e NNTP para e-mails de entrada e SMTP para e-mails de saída) independentemente do cliente de e-mail utilizado. O programa inclui plug-ins para os clientes de e-mail mais populares (Microsoft Office Outlook, Microsoft Outlook Express (Programa de e-mail do Windows) e o The Bat!) e suporta a desinfecção das suas bases de dados de e-mail.
- **Análise, em tempo real, do tráfego de Internet** transferido via HTTP.
- **Protecção do sistema de ficheiros**: análise Anti-Vírus de ficheiros individuais, directórios ou unidades. Para além disso, a aplicação pode efectuar análises Anti-Vírus exclusivamente para áreas críticas do sistema operativo e objectos de arranque do Microsoft Windows.
- **Protecção pró-activa**: o programa faz a monitorização constante da actividade das aplicações e processos a decorrer na memória de

acesso aleatório (RAM), impedindo alterações perigosas ao sistema de ficheiros e registo e restaura o sistema após influência maliciosa.

A **Protecção contra fraude na Internet** é garantida devido à capacidade de reconhecer ataques de "phishing", o que ajuda a prevenir fugas de dados confidenciais (primeiro de tudo, das suas passwords, números da conta bancária e cartões de crédito) e bloqueia a execução de scripts perigosos nas páginas de Internet, janelas que se abram (pop-up) e faixas publicitárias (banners). A funcionalidade **bloquear chamadas telefónicas a pagar no destino** ajuda a identificar o software que tenta usar o modem para ligação secreta não-autorizada a serviços de telefone pagos e previne essa actividade. O módulo de *Controlo de Privacidade* mantêm seguras as suas informações confidenciais em relação ao acesso e transmissão não autorizados. O *Controlo Parental* é uma componente do Kaspersky Internet Security que monitoriza o acesso dos utilizadores à Internet.

O Kaspersky Internet Security 7.0 **regista tentativas de procura de portas do computador**, que frequentemente precedem ataques de rede e defende efectivamente contra ataques típicos de hackers. O programa usa as **regras definidas como base** para controlo de todas as transacções de rede, analisando todos os **pacotes de dados de entrada e de saída**. O **Modo Furtivo** (devido à tecnologia SmartStealth™) **impede a detecção do computador a partir do exterior**. Quando muda para esse modo, o sistema bloqueia toda a actividade de rede, excepto algumas transacções permitidas por regras definidas pelo utilizador.

O programa emprega uma abordagem complexa da filtragem anti-spam de e-mails de entrada:

- Verificação de listas negras e brancas de destinatários (incluindo endereços de sites de phishing).
- Inspecção de frases no corpo da mensagem.
- Análise do texto da mensagem usando um algoritmo de auto-aprendizagem.
- Reconhecimento de spam enviado em ficheiros de imagem.

Kaspersky Anti-Virus Mobile

O Kaspersky® Anti-Virus Mobile fornece protecção Anti-Vírus para dispositivos móveis com os sistemas operativos Symbian OS e Microsoft Windows Mobile. O programa fornece uma protecção Anti-Vírus abrangente, incluindo:

- **Verificação (sob pedido)** da memória do dispositivo móvel, cartões de memória, pastas individuais ou ficheiros específicos. Se for detectado um ficheiro infectado, este é movido para a pasta da Quarentena ou é apagado.

- **Verificação em tempo real -** analisa automaticamente todos os ficheiros de entrada ou saída, assim como ficheiros quando são efectuadas tentativas para lhes aceder.
- **Protecção em relação a spam em mensagens de texto**.

Kaspersky Anti-Virus para Servidores de Ficheiros

Este pacote de software fornece protecção credível para os sistemas de ficheiros em servidores com os sistemas operativos Microsoft Windows, Novell NetWare, Linux e Samba, em relação a todo o tipo de software malicioso. O pacote inclui as seguintes aplicações da Kaspersky Lab:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus para Windows Server.
- Kaspersky Anti-Virus para Linux File Server.
- Kaspersky Anti-Virus para Novell Netware.
- Kaspersky Anti-Virus para Samba Server.

Características e funcionalidade:

- *Protege os sistemas de ficheiros de servidores em tempo real*: Todos os ficheiros do servidor são analisados quando abertos ou guardados no servidor.
- *Impede surtos de vírus*.
- *Verificações sob pedido* de todo o sistema de ficheiros ou ficheiros e pastas individuais.
- *Uso de tecnologias de optimização* ao verificar objectos no sistema de ficheiros do servidor.
- *Reversão do sistema após ataques de vírus*.
- *Escalabilidade do pacote de software* no âmbito dos recursos de sistema disponíveis.
- *Monitorização do equilíbrio de carga do sistema*.
- *Criação de uma lista de processos confiáveis* cuja actividade no servidor não é sujeita ao controlo pelo pacote de software.
- *Administração remota* do pacote de software, incluindo instalação, configuração e administração centralizada.
- *Armazenamento de cópias de segurança de objectos infectados ou apagados* caso necessite de restaurá-los.

- *Colocação na quarentena* de objectos suspeitos.
- *Envio, ao administrador do sistema, de notificações sobre eventos* no funcionamento do programa.
- *Registo de relatórios detalhados*.
- *Actualização automática* das bases de dados do programa.

Kaspersky Open Space Security

O Kaspersky Open Space Security é um pacote de software com uma nova abordagem de segurança para as redes empresariais actuais de qualquer dimensão, fornecendo a protecção centralizada dos sistemas de informação e suporte para escritórios remotos e utilizadores de telemóveis.

O pacote inclui quatro programas:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

As especificidades de cada programa são apresentadas de seguida.

Kaspersky WorkSpace Security é um programa para a protecção centralizada de estações de trabalho no interior e no exterior das redes empresariais, relativamente às actuais ameaças da Internet (vírus, spyware, ataques de hacker e spam).

Características e funcionalidade:

- *Protecção abrangente em relação a vírus, spyware, ataques de hacker e spam*.
- *Defesa Pró-activa* em relação a novos programas maliciosos cujas assinaturas ainda não foram adicionadas à base de dados.
- *Firewall Pessoal* com sistema de detecção de intrusões e avisos de ataques de rede.
- *Reversão para alterações maliciosas ao sistema*.
- *Protecção em relação a ataques de phishing e lixo electrónico*.
- *Redistribuição dinâmica de recursos* durante verificações completas do sistema.

- *Administração remota* do pacote de software, incluindo instalação, configuração e administração centralizada.
- *Suporte para Cisco® NAC* (*Controlo de Admissão de Rede*).
- *Verificação de tráfego de e-mail e de Internet* em tempo real.
- *Bloqueio de janelas de popup e faixas publicitárias (banner ads)* quando navega na Internet.
- *Funcionamento seguro em qualquer tipo de rede*, incluindo Wi-Fi.
- *Ferramentas de criação de disco de recuperação* que permitem restaurar o seu sistema após um surto de vírus.
- *Sistema alargado de relatórios* sobre o estado de protecção.
- *Actualizações automáticas das bases de dados*.
- *Suporte total para sistemas operativos de 64-bit*.
- *Optimização do desempenho do programa em portáteis* (Intel® Centrino® Duo technology).
- *Função de desinfecção remota* (Intel® Active Management, Intel® vPro™).

Kaspersky Business Space Security fornece uma protecção óptima dos recursos de informação da sua empresa em relação às actuais ameaças da Internet. O Kaspersky Business Space Security protege as estações de trabalho e servidores de ficheiros em relação a todos os tipos de vírus, Trojans e worms, impede surtos de vírus e protege a informação ao mesmo tempo que fornece acesso rápido aos recursos da rede, por parte dos utilizadores.

Características e funcionalidade:

- *Administração remota do pacote de software*, incluindo instalação, configuração e administração centralizada.
- *Suporte para Cisco® NAC* (Controlo de Admissão de Rede).
- *Protecção das estações de trabalho e servidores de ficheiros em relação a todos os tipos de ameaças da Internet*.
- *Tecnologia iSwift para evitar a repetição da verificação de ficheiros na rede*.
- *Distribuição de carga entre os processadores do servidor*.

- *Colocação na quarentena de objectos suspeitos* de estações de trabalho.
- *Reversão para alterações maliciosas ao sistema*.
- *Escalabilidade do pacote de software* no âmbito dos recursos de sistema disponíveis.
- *Defesa Pró-activa* para estações de trabalho em relação a novos programas maliciosos cujas assinaturas ainda não foram adicionadas à base de dados.
- *Verificação de tráfego de e-mail e de Internet* em tempo real.
- *Firewall Pessoal* com sistema de detecção de intrusões e avisos de ataques de rede.
- *Protecção enquanto utiliza redes Wi-Fi*.
- *Autodefesa* em relação a programas maliciosos.
- *Colocação na quarentena* de objectos suspeitos.
- *Actualizações automáticas das bases de dados*.

Kaspersky Enterprise Space Security

Este programa inclui componentes para proteger estações de trabalho e servidores ligados, em relação a todas as ameaças actuais da Internet. Apaga vírus de e-mails, mantendo a informação segura, ao mesmo tempo que fornece acesso seguro aos recursos da rede, por parte dos utilizadores.

Características e funcionalidade:

- *Protecção das estações de trabalho e servidores de ficheiros em relação a vírus, Trojans e worms*.
- *Protecção dos servidores de e-mail Sendmail, Qmail, Postfix e Exim*.
- *Verificação de todos os e-mails no Microsoft Exchange Server*, incluindo pastas partilhadas.
- *Processamento de e-mails, bases de dados e outros objectos para os servidores Lotus Domino*.
- *Protecção em relação a ataques de phishing e lixo electrónico*.
- *Impede o envio em massa de e-mails e surtos de vírus*.

- *Escalabilidade do pacote de software* no âmbito dos recursos de sistema disponíveis.
- *Administração remota do pacote de software*, incluindo instalação, configuração e administração centralizada.
- *Suporte para Cisco® NAC* (Controlo de Admissão de Rede).
- *Defesa pró-activa* para estações de trabalho, em relação a novos programas maliciosos cujas assinaturas ainda não foram adicionadas à base de dados.
- *Firewall Pessoal* com sistema de detecção de intrusões e avisos de ataques de rede.
- *Funcionamento seguro ao utilizar redes Wi-Fi*.
- *Verificação de tráfego de Internet* em tempo real.
- *Reversão para alterações maliciosas ao sistema*.
- *Redistribuição dinâmica de recursos* durante verificações completas do sistema.
- *Colocação na quarentena* de objectos suspeitos.
- *Sistema alargado de relatórios* sobre o estado de protecção.
- *Actualizações automáticas das bases de dados*.

Kaspersky Total Space Security

Esta solução monitoriza todos os fluxos de dados de entrada e de saída (e-mail, Internet e todas as interacções de rede). Inclui componentes para proteger estações de trabalho e dispositivos móveis, mantém a informação segura, ao mesmo tempo que fornece acesso seguro aos recursos de informação da empresa e da Internet, por parte dos utilizadores e garante comunicação segura por e-mail.

Características e funcionalidade:

- *Protecção abrangente em relação a vírus, spyware, ataques de hacker e spam* em todos os níveis da rede empresarial, desde as estações de trabalho à portas de ligação da Internet.
- *Defesa pró-activa* para estações de trabalho, em relação a novos programas maliciosos cujas assinaturas ainda não foram adicionadas à base de dados.
- *Protecção dos servidores de e-mail e servidores ligados*.

- *Verificação de tráfego de Internet* (HTTP/FTP) em tempo real, à entrada da rede local.
- *Escalabilidade do pacote de software* no âmbito dos recursos de sistema disponíveis.
- *Bloqueio do acesso a partir de estações de trabalho infectadas*.
- *Impede surtos de vírus*.
- *Relatórios centralizados sobre o estado de protecção*.
- *Administração remota do pacote de software*, incluindo instalação, configuração e administração centralizada.
- *Suporte para Cisco® NAC* (Controlo de Admissão de Rede).
- *Suporte para servidores proxy de hardware*.
- *Filtragem do tráfego de Internet* através de uma lista confiável de servidores, tipos de objectos e grupos de utilizadores.
- *Tecnologia iSwift para evitar a repetição da verificação de ficheiros* na rede.
- *Redistribuição dinâmica de recursos* durante verificações completas do sistema.
- *Firewall Pessoal* com sistema de detecção de intrusões e avisos de ataques de rede.
- *Funcionamento seguro para utilizadores em qualquer tipo de rede*, incluindo Wi-Fi.
- *Protecção em relação a ataques de phishing e lixo electrónico*.
- *Função de desinfecção remota* (Intel® Active Management, Intel® vPro™).
- *Reversão para alterações maliciosas ao sistema*.
- *Autodefesa* em relação a programas maliciosos.
- *Suporte total para sistemas operativos de 64-bit*.
- Actualizações automáticas das bases de dados.

Kaspersky Security para Servidores de E-mail

Este programa serve para proteger os servidores de e-mail e servidores ligados, em relação a programas maliciosos e spam. O programa inclui aplicação para proteger todos os servidores de e-mail típicos (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix e Exim) e também lhe permite configurar uma porta de ligação dedicada para e-mail. A solução inclui:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus para Lotus Notes/Domino.
- Kaspersky Anti-Virus para Microsoft Exchange.
- Kaspersky Anti-Virus para Linux Mail Server.

As suas características incluem:

- *Protecção credível em relação a programas maliciosos ou potencialmente perigosos*.
- *Filtragem de lixo electrónico*.
- *Verificação de e-mails de entrada e de saída e respectivos anexos*.
- *Verificação de todos os e-mails no Microsoft Exchange Server, quanto à presença de vírus*, incluindo pastas partilhadas.
- *Processa e-mails, bases de dados e outros objectos para os servidores Lotus Notes/Domino*.
- *Filtra e-mails por tipo de anexo*.
- *Coloca na quarentena* objectos suspeitos.
- *Sistema de administração fácil de utilizar* para o programa.
- *Impede surtos de vírus*.
- *Monitoriza o estado de protecção do sistema*, utilizando notificações.
- *Sistema de relatórios* sobre o funcionamento do programa.
- *Escalabilidade do pacote de software* no âmbito dos recursos de sistema disponíveis.
- *Actualização automática das bases de dados*.

Kaspersky Security para Portas de Ligação da Internet

Este programa fornece acesso seguro à Internet para todos os funcionários de uma organização, apagando automaticamente o software malicioso e potencialmente perigoso nos dados de entrada por HTTP/FTP. A solução inclui:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus para Proxy Server.
- Kaspersky Anti-Virus para Microsoft ISA Server.
- Kaspersky Anti-Virus para Check Point FireWall-1.

As suas características incluem:

- *Protecção credível em relação a programas maliciosos ou potencialmente perigosos*.
- *Verificação de tráfego de Internet* (HTTP/FTP) em tempo real.
- *Filtragem do tráfego de Internet* através de uma lista confiável de servidores, tipos de objectos e grupos de utilizadores.
- *Coloca na quarentena* objectos suspeitos.
- *Sistema de administração fácil de utilizar*.
- *Sistema de relatórios* sobre o funcionamento do programa.
- *Suporte para servidores proxy de hardware*.
- *Escalabilidade do pacote de software* no âmbito dos recursos de sistema disponíveis.
- *Actualização automática das bases de dados*.

Kaspersky® Anti-Spam

O Kaspersky® Anti-Spam é uma solução de software pioneira que foi desenhada para ajudar organizações com redes de pequena e média dimensão na guerra contra a invasão de e-mails indesejados (spam). O produto combina a tecnologia revolucionária da análise linguística com os métodos modernos de filtragem de e-mails, incluindo as Listas Negras de DNS e características de cartas formais. A sua combinação única de serviços permite ao utilizador identificar e eliminar até 95% de tráfego indesejado.

Instalado à entrada de uma rede, onde monitoriza, em termos de spam, os fluxos de tráfego de e-mails de entrada, o Kaspersky® Anti-Spam actua como uma barreira contra os e-mails não solicitados. O produto é compatível com qualquer sistema de e-mail e pode ser instalado num servidor de e-mail já existente ou num servidor dedicado.

O elevado desempenho do Kaspersky® Anti-Spam é garantido pelas actualizações diárias da base de dados de filtragem de conteúdos, adicionando amostras fornecidas pelos especialistas laboratoriais de linguística. As bases de dados são actualizadas a cada 20 minutos.

Kaspersky Anti-Virus® para MIMESweeper

O Kaspersky® Anti-Virus para MIMESweeper fornece uma verificação, de alta velocidade, do tráfego de SMTP nos servidores que usam o Clearswift MIMEsweeper para SMTP / Clearswift MIMEsweeper para Exchange / Clearswift MIMEsweeper para Internet.

O programa é um plug-in e efectua verificações de vírus e processa, em tempo real, o tráfego de e-mails de entrada e de saída.

B.2. Contacte-nos

Se tiver quaisquer questões, comentários ou sugestões, remeta-as a um dos nossos distribuidores ou, directamente, à Kaspersky Lab. Ficaremos gratos em ajudá-lo por telefone ou por e-mail em qualquer assunto relacionado com o nosso produto. Tenha a certeza de que todas as suas recomendações e sugestões serão amplamente revistas e consideradas.

Suporte técnico	Pode encontrar informação de suporte técnico em http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html
Informação Geral	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: info@kaspersky.com

APÊNDICE C. CONTRATO DE LICENÇA

Contrato de licença de utilizador final

NOTA PARA TODOS OS UTILIZADORES: LEIA CUIDADOSAMENTE O SEGUINTE CONTRATO LEGAL ("CONTRATO") PARA A LICENÇA DO KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS SERVERS ("SOFTWARE") PRODUZIDO PELA KASPERSKY LAB ("KASPERSKY LAB").

SE COMPROU ESTE SOFTWARE PELA INTERNET FAZENDO CLIQUE NO BOTÃO PARA ACEITAR, VOCÊ (TANTO COMO INDIVÍDUO OU COMO ENTIDADE LEGAL ÚNICA) CONSENTE EM ACEITAR E A SER PARTE DESTE CONTRATO. SE NÃO CONCORDAR COM TODOS OS SEUS TERMOS NESTE CONTRATO, CLIQUE NO BOTÃO QUE INDICA QUE NÃO ACEITA OS TERMOS DESTE CONTRATO, E NÃO INSTALE O SOFTWARE.

SE TIVER COMPRADO ESTE SOFTWARE NUM MEIO FÍSICO, TIVER ROMPIDO O ENVELOPE DO CD VOCÊ (TANTO COMO INDIVÍDUO OU COMO ENTIDADE LEGAL ÚNICA) CONSENTE EM ESTAR LIGADO A ESTE CONTRATO. SE NÃO CONCORDAR COM TODOS OS TERMOS DESTE CONTRATO NÃO ROMPA O ENVELOPE DO CD, DESCARREGUE, INSTALE OU USE ESTE SOFTWARE.

SEGUNDO A LEGISLAÇÃO, REFERENTE AO SOFTWARE KASPERSKY DESTINADO A UTILIZADORES INDIVIDUAIS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY PARA PDA) COMPRADO ONLINE NA PÁGINA WEB DA KASPERSKY LAB, O CLIENTE DEVE TER UM PERÍODO DE SETE DIAS ÚTEIS DESDE A ENTREGA DO PRODUTO PARA O DEVOLVER AO COMERCIANTE PARA TROCA OU REEMBOLSO, DESDE QUE ESTE SOFTWARE NÃO TENHA O SELO DESTRUÍDO.

RELATIVAMENTE AO SOFTWARE KASPERSKY DESTINADO A CONSUMIDORES INDIVIDUAIS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY PARA PDA) NÃO ADQUIRIDO ONLINE PELA INTERNET, ESTE SOFTWARE NÃO PODE SER DEVOLVIDO NEM TROCADO, EXCEPTO EM CASO DE CONSIDERAÇÕES EM CONTRÁRIO PELO PARCEIRO QUE VENDE O PRODUTO. NESTE CASO, A KASPERSKY LAB NÃO FICA ABRANGIDA PELAS CLÁUSULAS DO PARCEIRO.

O DIREITO A DEVOLUÇÃO E REEMBOLSO ABRANGE APENAS O COMPRADOR ORIGINAL.

1. *Concessão de licença*. Sujeito ao pagamento de taxas de licença aplicáveis, e sujeito aos termos e condições deste Contrato, a Kaspersky Lab concede-lhe por este meio o direito não-exclusivo e intransmissível a usar uma cópia da versão especificada do Software e a documentação acompanhante (a "Documentação") para o termo deste Contrato apenas para os fins internos de negócio.

1.1 *Utilização*. O número de computadores que o Utilizador pode proteger com o Software está especificado no Ficheiro de Chave de Licença e indicado na janela “Serviço”. O Software não pode ser utilizado para proteger redes com mais do que este número de servidores de ficheiros.

1.1.1 O software está "em utilização" num dispositivo cliente quando estiver carregado na memória temporária (ou seja, memória de acesso aleatório ou RAM) ou instalado na memória permanente (por exemplo, disco rígido, CD-ROM, ou outro meio de armazenamento) desse dispositivo cliente. Esta licença autoriza-o a fazer apenas as cópias de segurança necessárias do software para seu uso legal e apenas para fins de cópia de segurança, desde que todas essas cópias contenham todos os avisos proprietários do software. Deverá manter registos do número e localização de todas as cópias do software e documentação e tomar todas as precauções razoáveis para proteger o software de cópias ou utilização não-autorizadas.

1.1.2 O Software protege o computador em relação a vírus cujas assinaturas estão contidas na base de dados de assinaturas de ameaças que está disponível nos servidores de actualização da Kaspersky Lab.

1.1.3 Se vender o dispositivo cliente onde o software está instalado, deverá assegurar que todas as cópias do software foram previamente apagadas.

1.1.4 Não deve descompilar, proceder a engenharia reversa, desmontar ou reduzir de outro modo qualquer parte deste software numa forma humanamente legível nem permitir a terceiros que o façam. A interface de informação necessária para obter interoperacionalidade do software com programas de computador criados independentemente será fornecida pela Kaspersky Lab a pedido mediante pagamento dos seus custos razoáveis e despesas de obtenção e fornecimento dessa informação. Em caso de a Kaspersky Lab o notificar que não pretende tornar essa informação disponível por qualquer razão, incluindo (sem limitação) os custos, deverá ser-lhe permitido dar os passos para obter interoperacionalidade, desde que apenas proceda a engenharia reversa ou descompile o software na medida permitida por lei.

1.1.5 Não deverá executar correcções de erros, ou modificar de outro modo, adaptar, ou traduzir o software, nem criar trabalhos derivativos do software, nem permitir a terceiros copiar o software (além do aqui expressamente permitido).

1.1.6 Não deve alugar, ceder em leasing ou emprestar o software a qualquer outra pessoa, nem transferir ou sublicenciar os seus direitos de licença a qualquer pessoa.

1.1.7 Não deve usar o software em ferramentas automáticas, semi-automáticas ou manuais concebidas para criar assinaturas de vírus, rotinas de detecção de vírus, quaisquer outros dados ou código para detecção de código malicioso ou dados.

1.1.8 A Kaspersky Lab pode pedir ao Utilizador para instalar a última versão do Software (a última versão e o último pacote de manutenção).

1.1.9 Remoção de Produtos Potencialmente Nocivos. Você reconhece e concorda que, para além da detecção de software nocivo e malicioso, o Produto também pode identificar, remover e/ou desactivar produtos potencialmente nocivos, incluindo aqueles que são considerados ou classificados como Adware (software com publicidade), Riskware (software potencialmente perigoso), Pornware (software com pornografia), etc.

2. *Suporte*.

(i) A Kaspersky Lab fornecerá os serviços de suporte ("Serviços de Suporte"), tal como está definido abaixo, por um período, especificado no Ficheiro de Chave de Licença e indicado na janela "Serviço", desde o momento da activação após:

   (a) Pagamento do montante corrente de suporte à altura, e:

   (b) O serviço de suporte técnico da Kaspersky Lab também tem direito a exigir um registo adicional do Utilizador Final para efeitos de atribuição de identificador para a prestação de Serviços de Suporte.

   (c) Até à activação do Software e/ou obtenção de identificador do Utilizador Final (ID Cliente), o serviço de suporte técnico apenas presta assistência na activação do Software e no registo do Utilizador Final.

(ii) Ao preencher o formulário de subscrição dos serviços de suporte dará consentimento aos termos da política de privacidade da Kaspersky Lab, que está presente em www.kaspersky.com/privacy, e consente explicitamente com a transferência de dados de outros países fora do seu como está definido na Política de Privacidade.

(iii) Os serviços de suporte terminarão a menos que sejam renovados anualmente por pagamento do montante para suporte anual à altura e por preenchimento do formulário de subscrição dos serviços de suporte de novo.

(iv) "Serviços de suporte" significa:

   (a) Actualizações horárias da base de dados Anti-Vírus;

(b) Actualizações livres de software, incluindo actualizações de versão;

(c) Suporte técnico alargado por e-mail e linha telefónica fornecida pelo vendedor e/ou revendedor;

(d) Actualizações de detecção de vírus e desinfecção durante 24 horas por dia.

(v) Os Serviços de Suporte são fornecidos apenas se e quando possuir a última versão do Software (incluindo pacotes de manutenção) instalada no seu computador, tal como está disponível no site oficial da Kaspersky Lab (www.kaspersky.com).

3. *Direitos de propriedade*. O software está protegido por leis de direito de cópia. A Kaspersky Lab e seus fornecedores detém e retêm todos os direitos, títulos e interesse pelo software, incluindo todos os direitos de autor, patentes, marcas registadas e outros direitos de propriedade intelectual nele. A sua posse, instalação, ou utilização do software não transfere qualquer título à propriedade intelectual no software para si, e não adquire quaisquer direitos ao software excepto os definidos neste Contrato.

4. *Confidencialidade*. Concorda que o software e a documentação, incluindo a concepção específica e estrutura de programas individuais e do ficheiro de identificação de licença, constituem informação confidencial exclusiva da Kaspersky Lab. Não deve revelar, fornecer, ou disponibilizar de outra forma essa informação confidencial nalguma forma a terceiros sem o consentimento prévio da Kaspersky Lab. Deverá implementar medidas razoáveis de segurança para proteger essa informação confidencial, mas sem limitação ao exposto deverá adoptar as melhores medidas para manter a segurança do código de activação.

5. *Garantia Limitada*.

(i) A Kaspersky Lab garante que pelos (6) meses desde a primeira transferência ou instalação do Software comprado num meio físico deverá operar substancialmente em consonância com a funcionalidade descrita na Documentação quando for adequadamente utilizado e do modo especificado na Documentação.

(ii) Aceitará toda a responsabilidade pela selecção deste software para obedecer aos seus requisitos. A Kaspersky Lab não garante que o software e/ou a documentação seja apropriada a esses requisitos nem que qualquer uso seja ininterrupto ou livre de erros.

(iii) A Kaspersky Lab não garante que este software identifique todos os vírus conhecidos e cartas de spam, nem que o software não aponte eventualmente um vírus erradamente num título não infectado por esse vírus.

(iv) A Kaspersky Lab não garante que este Software forneça protecção depois da data de validade (ver section.2 (i))

(v) A sua única solução e toda a responsabilidade da Kaspersky Lab pela quebra da garantia no parágrafo (i) será opção da Kaspersky Lab, para reparar, trocar ou reembolsar o software se for relatado à Kaspersky Lab ou sua designada durante o período de garantia. Deverá fornecer toda a informação consoante o necessário para assistir o fornecedor a resolver o item defeituoso.

(vi) A garantia em (i) não se deve aplicar se você tiver (a) feito ou causado quaisquer modificações a este software sem o consentimento da Kaspersky Lab, (b) usar o software de um modo para o qual não foi destinado, ou (c) usar o software além do permitido neste Contrato.

(vii) As garantias e condições definidas neste Contrato sobrepõem-se a todas as outras condições, garantias ou outros termos respeitantes ao fornecimento ou intenção de fornecimento, falta de fornecimento ou atraso em fornecer o software ou a documentação que deveria, mas para este parágrafo (vi) tem efeito entre a Kaspersky Lab e o cliente ou seria de outro modo implicado ou incluído neste Contrato ou qualquer contrato colateral, quer por estatuto, lei comum ou de outra forma, todos aqui excluídos (incluindo, sem limitação, as condições implicadas, garantias ou outros termos como qualidade satisfatória, capacidade para o fim adequado ou como utilização de perícia razoável e cuidado).

6. *Limitação de responsabilidade*.

(i) Nada neste Contrato deverá excluir ou limitar a responsabilidade da Kaspersky Lab por (a) prejuízo de fraude, (b) morte ou acidente pessoal causado pela sua quebra de dever comum legal de cuidado ou qualquer quebra negligente de um termo deste Contrato, ou (c) qualquer outra responsabilidade que não possa ser excluída por lei.

(ii) Sujeito ao parágrafo (i) acima, o fornecedor não deverá ter nenhuma responsabilidade (se em contrato, prejuízo, restituição ou de outra forma) por qualquer dos seguintes prejuízos ou danos (se esses prejuízos ou danos foram previstos, previsíveis, conhecidos ou em contrário):

(a) Perda de rendimento;

(b) Perda actual ou antecipada de lucros (incluindo perda de lucros em contratos);

(c) Perda da utilidade do dinheiro;

(d) Perda de economias antecipadas;

(e) Perda de negócio;

(f) Perda de oportunidade;

(g) Perda de valor da empresa;

(h) Perda de reputação;

(i) Perda de, danos a ou corrupção de dados, ou:

(j) Qualquer perda indirecta ou em consequência ou danos de alguma forma provocados (incluindo, para evitar dúvida, onde tal perda ou dano é do tipo especificado nos parágrafos (ii), (a) a (ii), (i).

(iii) Sujeito ao parágrafo (i), a responsabilidade da Kaspersky Lab (quer seja em contrato, prejuízo, restituição ou noutra forma) resultante de ou em ligação com o fornecimento do software não pode em caso algum exceder uma soma igual ao montante pago igualmente por si pelo Software.

7. Este Contrato contém o estipulado completo entre as partes no que respeita à matéria de assunto aqui feita e sobrepõe-se a todo e qualquer estipulado prévio, compromissos e promessas entre si e a Kaspersky Lab, quer orais ou por escrito, que foram concedidas ou podem estar implicadas por qualquer escrito ou dito em negociações entre nós ou o nosso representante antes deste Contrato, e todos os contratos prévios entre as partes relacionados com os assuntos anteriormente referidos deverão cessar para ter efeito desde a Data Efectiva.

Quando utilizar o software de demonstração, não tem direito ao Suporte Técnico especificado na Cláusula 2 deste CLUF, nem tem direito a vender a cópia que possui a outras partes.

Tem direito a utilizar o software para efeitos de demonstração pelo período de tempo especificado no ficheiro de chave de licença, a contar do momento de activação (este período pode ser visualizado na janela Serviço da Interface Gráfica do Utilizador do software).